Data Collection for Security Measurement in Wireless Sensor Networks: A Survey

Haomeng Xie, Zheng Yan, *Senior Member, IEEE*, Zhen Yao and Mohammed Atiquzzaman, *Senior Member, IEEE*

Abstract—Wireless Sensor Network (WSN) is an indispensible part of IoT that has been applied in many fields to monitor environments and collect data from surroundings. However, WSNs are highly susceptible to attacks due to its unique characteristics: large-scale, self-organization, dynamic topology and constrained resources. A number of systems have been proposed to effectively detect varieties of attacks in WSNs. However, most previous surveys on WSN attacks focus on detection methods for only one or two types of attacks and lack detailed performance analysis. Additionally, the literature lacks comprehensive studies on security-related data (in short security data) collection in WSNs. In this paper, we first provide an overview of WSNs and classify the attacks in WSNs based on protocol stack layers. For the purpose of WSN security measurement, we then research attack detection methods of eleven mainstream attacks. We extract security data that play an important role for detecting security anomaly towards security measurement. We further elaborate the advantages and disadvantages of the existing detection methods based on a number of evaluation criteria. Finally, we highlight a number of open problems in this research field based on our thorough survey and conclude this paper with possible future research directions.

Index Terms—attack detection, Internet of Things (IoT), security data collection, security measurement, Wireless Sensor Network (WSN),

1 Introduction

Internet of Things (IoT) plays a crucial role in realizing intelligent identification, positioning, tracking, monitoring and environment management. Through two-dimensional code reading devices, radio frequency identification (RFID) devices, infrared sensors, Global Position System (GPS), laser scanners, cloud storage and other network equipment, IoT connects the things in the physical world and the cyber world together and makes human life comfortable and convenient; thanks to many IoT intelligent applications supported by Wireless Sensor Networks (WSNs). WSN is an indispensable part of IoT [5], which is used by many IoT applications to monitor an environment and record its conditions, such as smart city [1], disaster warning, smart home [3] and intelligent healthcare [4].

However, WSN is very vulnerable to many attacks due to its unique characteristics: large-scale, self-organization, dynamic topology and constrained resources. WSN attacks may cause network anomalies that can be reflected in the data collected from the network. These collected data are valuable and can be used to detect network attacks. We define these data as security-related data, in short security data, since they can help us detect anomalies and figure out security threats, intrusions and attacks. Security data are generally generated in various kinds of WSN applications (e.g., smart city, smart home and intelligent healthcare). Depending on different detection methods, some security data are general sensory data (e.g., Received Signal Strength Indicator, acknowledgement messages, etc.), while some other security data are special data (e.g., fingerprint) that need to be extracted specifically. Attack detection supports security defense for resisting intrusions and security threats in WSNs, thus it plays an important role in securing WSN. Summing up existing attack detection methods and related security data is significant for understanding the current state of arts in the field of attack detection and working forward to measure WSN security. However, few works in the literature comprehensively review the detection methods of mainstream attacks and relevant security data collection and analytics in WSN.

Although the methods to detect various attacks have been intensively researched and reported in the literature, none of them provide a thorough review on security data collection and data analytics for detecting mainstream attacks in WSNs. Some recent surveys focus on security data collection [93], [94] and data analytics in the Internet [92], Ad Hoc network [96], LTE/LTE-A network [97] and mobile phones [95], rather than WSN. Some surveys [6-8], [12] mainly focus on a limited number of typical attacks and lack detailed performance analysis under uniform criteria in WSN. Although the authors in [9], [10] explained all mainstream attacks in WSNs, they did not review the

- *H. M. Xie is with the State Key Laboratory of ISN, School of Cyber Engineering, Xidian University, Xi'an, China and the Key Lab of Information Network Security, Ministry of Public Security, Shanghai, China, E-mail: Birch_forest@163.com.*
- *Z. Yan is with the State Key Laboratory of ISN, School of Cyber Engineering, Xidian University, Xi'an, China and the Department of Communications and Networking, Aalto University, Espoo, Finland, E-mail: zyan@xidian.edu.cn; zheng.yan@aalto.fi.*
- *Z. Yao is with State Key Laboratory of ISN, School of Cyber Engineering, Xidian University, Xi'an, China, E-mail: 695154820@qq.com.*
- *M. Atiquzzaman is with the School of Computer Science, University of Oklahoma, Norman, USA, E-mail: Atiq@ou.edu.*

xxxx-xxxx/0x/$xx.00 © 200x IEEE Published by the IEEE Computer Society

TABLE 1
COMPARISON OF OUR SURVEY WITH OTHER EXISTING SURVEYS

Covered Topics	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[15]	Our survey
Summarize mainstream attacks	Y	Y	N	Y	Y	N	Y	Y	Y
Propose a set of evaluation criteria	N	N	N	N	N	N	N	N	Y
Review attack detection methods	Y	Y	Y	N	N	Y	Y	Y	Y
Analyze the performance of detection methods based on evaluation criteria	N	N	N	N	N	N	N	N	Y
Summarize security data	N	N	N	N	N	N	N	N	Y
Propose a number of open issues and future research trends	Y	N	N	N	N	Y	Y	Y	Y

methods to detect the attacks. Xie et al. [11] introduced detection methods according to the categorization of anomaly detection techniques other than protocol stack layers and attack types. They did not concern security data and did not evaluate performance based on a comprehensive set of criteria for data collection and analytics. Sen [15] presented a view of security issues, various possible attacks and corresponding countermeasures in WSN. However, none of them focus on abnormal detection through security data collection, processing and analytics in WSN. In general, the above-mentioned surveys lack following studies: (1) comprehensive studies on attack detection methods of mainstream security threats with attention to security data collection and analytics; (2) extensive analysis on detection methods based on a uniform set of criteria for security data collection and data analytics; and (3) synthetic attack detection in WSN.

The objective of this paper is to provide a survey on mainstream attack detection methods in WSNs, summarize security data used in the methods towards WSN security measurement in order to explore future research directions in this research field. We study the mainstream security threats in WSNs based on network layers and their corresponding detection methods. In order to analyze the performance of security data collection and attack detection methods, we propose a list of evaluation criteria to instruct our review on the performance of existing work and aid our judgement on future research trends. In our survey, we mainly focus on security data collection and data analytics for the purpose of setting up a holonomic attack detection system towards WSN security measurement. Security defense is not our focus since some papers [15], [16] have given a detailed summary and analysis on it.

Although we can find a number of existing surveys about attack detection and security defense in WSN, our survey has different focuses. We summarize security data according to different attacks, conduct literature evaluation based on a set of evaluation criteria. We carefully compare our survey with other existing surveys of attack detection and security defense in WSN in Table 1. Through comparison, we can summarize the main contributions of this paper as below:

- To the best of our knowledge, this is one of the first papers that give an extensive overview and detailed performance analysis of mainstream attack detection methods in WSNs. It summarizes security data used in these methods towards WSN security measurement.
- We propose a set of comprehensive evaluation criteria to analyze the performance of attack detection with a focus on security data collection and analytics.
- Besides security data collection and attack detection, we further review existing methods for detecting synthetic attacks.
- Based on detailed analysis and discussion, we find a number of open issues and forecast future research trends.

The rest of the paper is organized as follows. Section 2 introduces the special constraints of WSN, its layered architecture and the classification of WSN mainstream attacks. In Section 3, we propose a number of evaluation criteria for security data collection and attack detection in WSNs. Section 4 reviews attack detection methods in WSNs and discusses their advantages and disadvantages based on the proposed evaluation criteria. We also summarize the security data that are used in each method in the survey. Based on our thorough survey, we highlight open issues and propose future research directions in Section 5, followed by our concluding remarks in the last section.

2 CONSTRAINTS AND SECURITY THREATS

2.1 Special Constraints of WSNs

WSN is a resource-constrained network. Each sensor node in the WSN has limited resources regarding computation capacity, communication range and memory space and restricted energy.

Limited Energy: energy is one of the most important resources in the WSN. Energy in a sensor is mainly used for computation, communication and sensor transducer. However, the communication consumes the most energy in the WSN and every bit transmitted by a wireless sensor consumes the same energy as executing more than 200 clock cycles in CPU [13]. Thus, under the premise of accuracy, we should minimize communications to save energy in attack detection.

Memory constraint: memory is generally composed of flash memory and RAM in a sensor node. Flash memory is applied to store downloaded application codes and RAM is usually applied to store sensed data, intermediate computation and application programs. A sensor is so tiny that

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2883403, IEEE Internet of Things Journal

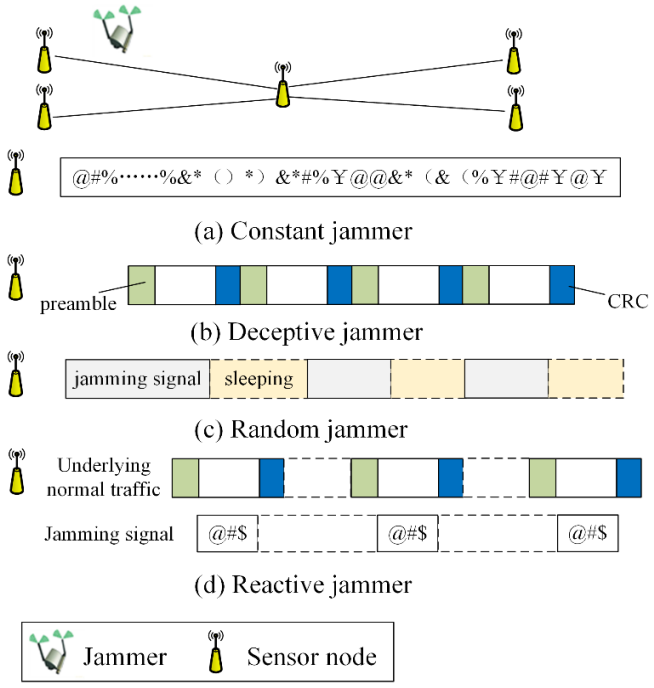

Fig. 1. Jamming attack models.

it has limited memory space and does not have enough memory to process big data and run complicated algorithms. For example, a common type of sensor TelosB only has 1MB (mega bytes) flash storage, 10KB (kilo bytes) RAM and 48KB (kilo bytes) program memory.

Transmission constraint: transmission constraint can be divided into three aspects: unreliable transmission, transmission latency and transmission range. Channel errors and packet collision may cause damage and loss of packets in an unreliable wireless channel. Furthermore, network congestion and multi-hop routing may lead to high latency. And actual transmission range mainly depends on energy and various environmental factors. Thus, we need to consider retransmission mechanisms, synchronization issues and data quality in attack detection.

2.2 Layered Architecture of WSNs

We give a taxology of attacks based on layered architecture of WSNs. The protocol stack of WSNs consists of five layers: physical layer, data link layer, network layer, transport layer and application layer.

(1) Physical Layer

The physical layer is responsible for providing a path to transmit binary bit streams by mean of frequency selection, carrier frequency generation, signal deflection, modulation and data encryption. Attacks on the WSN physical layer usually consists of eavesdropping attack, basic jamming attack, compromised node attack and replication node attack.

(2) Data Link Layer

The data link layer provides a reliable communication channel to neighbor nodes. In a MAC protocol, a node makes sure whether it can access to a communication channel by means of carrier sense, which is especially vulnerable to collision attack, intelligent jamming and denial-of-sleep attack.

(3) Network Layer

The network layer provides routing services to nodes. Attackers mainly launch attacks on routing, such as replay attack, Sybil attack, black hole attack, gray hole attack, wormhole attack, sinkhole attack, hello flooding attack and spoofing attack.

(4) Transport Layer

The transport layer is mainly used for setting up end-to-end connections and specifying reliable transport of packets, which is vulnerable to flooding attack and de-synchronization attack.

(5) Application Layer

The application layer is responsible for requesting and providing data for both individual sensor nodes and interactions with end users. It provides a variety of practical applications over WSNs. It is mainly vulnerable to attacks on reliability and malicious code attack [16] that have an adverse effect on application programs or nodes.

2.3 Security Threats in WSNs

In this subsection, we classify and give a brief introduction of the mainstream attacks in WSNs based on the layers targeted by the attacks

2.3.1 Attacks in Physical Layer

(1) Eavesdropping Attack

Eavesdropping attack is an activity that intercepts radio signals but does not destroy their integrity. It is a fundamental prerequisite of many other attacks. A malicious node monitors message transmission and intercepts it. If the message is not encrypted, the adversary can easily read it. It is a passive attack that can be scarcely detected if a malicious node has no other activities. But we can take advantage of effective protocols and encryption techniques to guard against this attack.

(2) Basic Jamming Attack

Jamming attack is an act that exploits electromagnetic energy to interfere or interrupt communications among legitimate nodes. It is generally divided into basic jamming attack and intelligent jamming attack. Basic jammer emits radio signals to prevent or disrupt data transmission. Xu et al. [19] divided jamming attacks into four taxonomies as described in Fig. 1. Constant jammer incessantly emits signals to hold up communication channels and prevents senor nodes from sending messages. Deceptive jammer incessantly emits regular packets without any intervals to deceive legitimate nodes into a receiving state so that they cannot send any messages. Random jammer converts between jamming and sleeping to save energy. Reactive jammer keeps quiet when there is no information in the channel and starts to attack as soon as it detects any channel activities. It prevents a receiver from receiving messages, and thus it is much harder to be detected. Constant jammer, random jammer and reactive jammer can launch basic jamming attack when they emit interference signals to sensor nodes.

(3) Compromised Node Attack

Compromised node [20] is an originally legitimate node that has been controlled by an adversary. The adversary can easily capture a sensor node in a sensitive security application of the WSN such as collecting data in a battlefield.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2883403, IEEE Internet of Things Journal

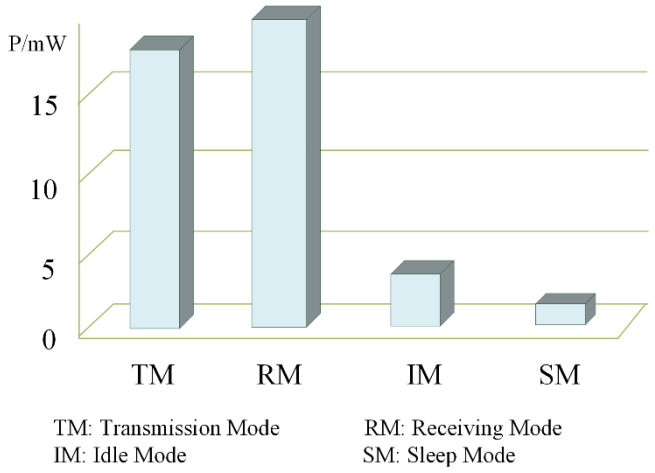

Fig. 2. Energy consumption of different modes.

Then the node is reprogrammed to launch various types of attacks.

(4) Replication Node Attack

The WSN may sometimes be exposed into an insecure environment, in which it is easy to reprogram a captured node and replicate it into a number of clones [21]. Because a replicated node has a legitimate identity such as a legitimate ID and keys inherited from the original node, it can take part in network operations as a normal node. It is difficult to detect this attack because replicated nodes can escape from all identity checks with legitimate IDs and keys. They may be distributed anywhere of the network and further launch insider attacks [23] to destroy the network. But it is not easy for an adversary to create a new legitimate node identity when the ID-based pair-wise keys are generated from a trusted authority [25].

2.3.2 Attacks in Data Link Layer

(1) Collision Attack

An attacker manages to distort byte values of each packet. As a result, a destination node will drop this packet because of checksum mismatch. Furthermore, persistent packet retransmission may consume a lot of resources

(2) Intelligent Jamming Attack

Intelligent jamming attack emits data packets that directly target known protocol rules, which can interfere communications and consume node energy. Only deceptive jammer, random jammer and reactive jammer can launch the intelligent jamming attack when they emit regular packets to sensor nodes.

(3) Denial-of-Sleep Attack

Energy is one of the most valuable resources in the WSN. There are several modes of sensor nodes for conserving energy as shown in Fig. 2 [68]. In this figure, the energy consumption of Sleep Mode is much less than that of other modes, so that it is better to keep sensor nodes in Sleep Mode rather than Idle Mode when no packet is sending or receiving to conserve energy. Just as its name implies, an attacker [26] prevents sensor nodes falling into a sleep and tries to exhaust power supply of them as quickly as possible. It may degrade the lifetime of sensor nodes and even break down network communications. Though some other attacks, such as jamming attack and flooding attack, can consume the energy of a sensor node, but denial-of-sleep attack is a clever attack that keeps a sensor node in an active mode and drain its battery more quickly.

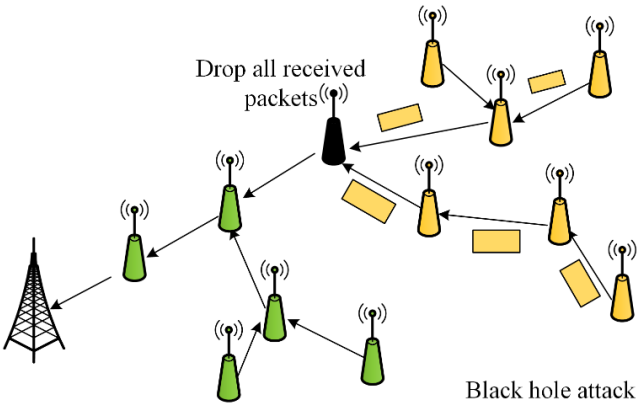

Fig. 3. Black hole attack.

2.3.3 Attacks in Network Layer

(1) Replay Attack

A malicious node catches packets that have been sent in WSN, and then replays them repeatedly to a legitimate node in order to consume its limited energy and dominate communication channels. The performance of the whole WSN will be impacted by this attack if network system design is poor.

(2) Sybil Attack

Newsome et al. [28] defined Sybil attack that a malicious node possesses multiple identities simultaneously and deceives normal nodes to believe that they have many neighbors. It has the ability to disrupt the integrity of network operations, such as distributed storage, routing [29], resource allocation, data aggregation, misbehavior detection and voting [28]. We can utilize a trusted center to verify identities of communication entities to prevent the Sybil attack, but this is not advisable in a distributed system.

(3) Black Hole Attack

Black hole attack [30], [31] is a type of denial of service (DoS) attack since it can result in zero packet delivery ratio and high propagation delay, as shown in Fig. 3. It often occurs close to a sink or a cluster head within one hop distance to attract more data packets. Or in the process of creating routing, a malicious node falsely replies RREP messages to deceive a source node that it has an immediate path to a destination node. Then it will swallow up all packets passing through it just like a black hole.

(4) Gray Hole Attack

Gray hole attack [32], [33] is also called selective forwarding attack, as shown in Fig. 4. It is a specific form of black hole attack as it only drops a part of packets. For example, it drops a packet every t seconds, or the packets with some sensitive information (e.g., sending to a specific destination).

(5) Wormhole Attack

Wormhole attack [34], [35] is a direct communication between at least two malicious nodes through a link with low latency and high efficiency, such as an effective wireless link or a hidden wired link. It captures packets in one part, transmits them to another part through its private link to distort an underlying routing protocol. It can attract a lot of honest nodes surrounding it to forward packets to it

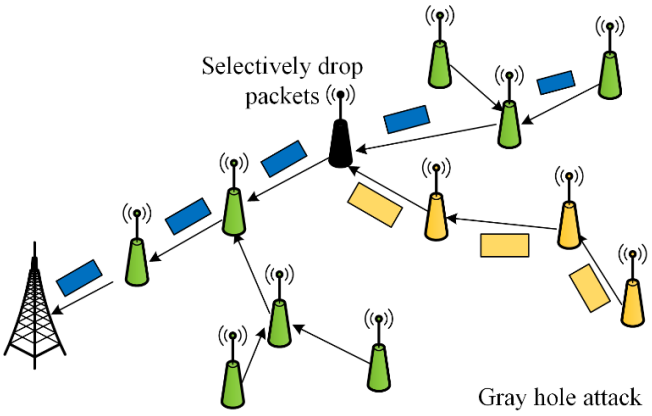

Fig. 4. Gray hole attack.

since it declares a nearest path to their destinations. Due to packet encapsulation technique, transmitting packets via malicious nodes does not increase hop counts, thus we cannot detect this attack through abnormal hop counts. This attack is easy to be launched because it does not need any cryptography techniques and compromised nodes to analyze data. This attack allows adversary to damage routing protocols, drop packets, or analyze the traffic flow later on. A simulation result in [36] illustrates that more than 50% of packets would be absorbed by malicious nodes and get discarded when there are more than two wormhole nodes in a network.

(6) Sinkhole Attack

A malicious node attracts as many traffic flows as possible around a sink using an efficient and powerful link, preventing the sink from receiving complete and valid packets. An adversary is attractive to surrounding nodes with an unfaithful routing. Neighbor nodes send information to a sink through the malicious node and the nodes that are near these neighbor nodes will be influenced by the adversary. This attack could collude with other attacks, such as wormhole attack to extent the sphere of influence or selective forwarding attack to drop some packets of great importance [37], [38].

(7) Hello Flooding Attack

Many routing protocols in the WSN use Hello messages to find neighbor nodes and create network communications. A node that receives a Hello message from another node is believed that it is in the radio range of the Hello message sender and therefore a neighbor of the sender [39]. For example, LEACH protocol [40] elects a cluster head based on a certain probability and residual energy. Then, the cluster head broadcasts Hello messages and nodes join the cluster after receiving the Hello message with a high Received Signal Strength Indicator (RSSI). An adversary could use a high-power transmitter to deceive a large area of nodes that are so far away from it to treat it as a neighbor, making them forward packets into oblivion.

(8) Spoofing Attack

An attacker can attract or suppress network traffic and generate false data by means of attracting, distorting and replaying routing information in this type of attack.

2.3.4 Attakcs in Transport Layer

(1) Flooding Attack

Flooding attack is such a kind of DoS attack that an attacker sends a large number of useless packets to a legitimate node in order to prevent it from normal communications and degrade network lifetime. For example, in TPC SYN flooding attack, an attacker sends a lot of connection establishment request packets to a victim. Once the victim receives them, it will reply acknowledgement packets to the demander and wait for connection. It also allocates storage space for transmission control. This attack prevents the network from working normally and occupies network resources.

(2) De-synchronization Attack

De-synchronization attack is a type of communication reliability attack. A reliable transport protocol must ensure that it can detect each packet loss, and each lost packet can be retransmitted until they reach its destination node. In the de-synchronization attack, an attacker forges packets with control flags or sequence numbers. Once a sensor node receives a bogus packet, it will request the sender to retransmit the lost packet. If this process continues, it will impact normal communications between source nodes and destination nodes, and consume a lot of energy.

2.3.5 Attacks in Application Layer

(1) Attack on Reliability

It is an attack that inserts malicious nodes between communication parties to generate false data or queries and increase energy consumption and collision.

(2) Malicious Code Attack

The adversary injects a worm in a node to disaggregate or gain complete control of the node, which can reduce the capability of the network and perform its intended functions.

2.3.6 Attacks across Multiple Layers

More than one previously defined attacks can be combined or launched in different layers of WSN protocol stack. These attacks include jamming attack, Denial of Service (DoS) attack and Man-in-the-Middle (MITM) attack.

(1) Jamming Attack

As mentioned before, jamming attack includes basic jamming attack in the physical layer and intelligent jamming attack in the data link layer.

(2) DoS Attack

In WSNs, the DoS attack not only consumes scarce resource of nodes, but also prevents legitimate users from accessing information or services. In the physical layer, the DoS attack can cause network congestion. Basic jamming attack is a kind of DoS attack. In the data link layer, attacker directly violates known communication protocols and transmits messages continually to generate collisions and result in packet retransmission and energy loss. Collision attack, intelligent jamming attack and denial-of-sleep attack belong to the DoS attack. In the network layer, malicious nodes refuse necessary routing information or send incorrect routing information to target nodes. Sybil attack, replay attack, black hole attack, grey hole attack, wormhole attack, sinkhole attack, hello flooding attack and spoofing attack all belong to the DoS attack. In the transport layer,

sensor nodes are vulnerable to flooding attack and de-synchronization attack that can generate a great number of connection and retransmission requests and consume a great deal of energy.

(3) Man-in-the-Middle Attack

It is an attack that an attacker secretly eavesdrops and possibly alters messages between two parties without their knowledge. Eavesdropping attack in the physical layer and replay attack in the network layer belong to MITM attack.

3 Evaluation Criteria for Security Data Collection in WSNs

In this section, we summarize a list of evaluation criteria to analyze the performance of security data collection and attack detection.

3.1 Criteria of Security Data Collection

3.1.1 Data Quality (DQ)

Data quality should be considered in security data collection. This is because wireless transmission is instable and wireless signal is susceptible to its environment. Radio communication is susceptible to many factors, such as context (geographical location, electromagnetic environments and climatic conditions), energy situation, multipath influence, transmission power and receiving sensitivity. A good and honest node could collect low quality data due to the influence of the above factors. An effective method should concern the above factors or some other influence factors seriously in order to ensure data quality. On the other hand, data quality should be measured, e.g., through quality-aware data aggregation. A data provider should be issued a higher weight if its collected data are closer to the aggregated results, and in return, its data should be counted more in the process of aggregation. Furthermore, privacy-preserving data quality measurement should also be investigated [98], [99], [100].

3.1.2 Data Trustworthiness (DT)

Data trustworthiness greatly impacts the quality of collected security data. Malicious nodes could insert false security data into networks and slander normal nodes. In addition, network dynamics (e.g., power exhaustion) can also affect the trustworthiness of data even though the nodes are honest. In this case, checkpoints (e.g., cluster heads and sinks) have responsibility to distinguish eligibility, legality and trustworthiness of security data to filter false data and protect normal nodes from being defamed by malicious nodes.

3.1.3 Effectiveness and Efficiency (EE)

Security data collection should have high effectiveness and efficiency in consideration of constrained energy and limited power in WSN nodes in order to extend their working time. We mainly take communication overhead into concern, because data transmission consumes the most energy in WSNs [14]. Computational complexity could also be considered with regard to security data processing if any. Communication overhead is mainly related to the size of communication data traffic. We stipulate the communication overhead of an effective data collection scheme is less than $\mathcal{O}(n^2)$, $\mathcal{O}(m^2 \times n)$, or $\mathcal{O}(k^2 \times n)$ since they are normal communication complexity in a network for all node-to-node communications, where n, m and k stand for the number of sensor nodes, neighbor nodes and checkpoint nodes, respectively.

3.1.4 Privacy (Pr)

The privacy of sensed data should not be exposed in the process of collecting security data. Otherwise, it may bring a great loss to related users. Once a malicious node obtains data, it may reveal the information of legitimate nodes. Sensor nodes' private information primarily consists of Location Privacy (LP) and Data Privacy (DP). LP means that the data cannot expose the location of source node, intermediate node or destination node to any unauthorized parties. A breach of location privacy may result in node capture or compromised node attack. In addition, extra and sensitive information may be collected in the process of data collection, so that we should seriously take DP into account.

3.1.5 Security Properties (SP)

A numnber of requirements should be ensured with regard to security data collection for attack detection, as specified below.

(1) Integrity

In the process of transmission and storage of data, we should ensure that the data are not tampered illegally. Thus, security data integrity should be satisfied.

(2) Confidentiality

Since security data are valuable, only legitimate sensor nodes can get the data. Thus, data confidentiality should be ensured, that is data contents should not be disclosed in the process of transmission.

(3) Non-repudiation

Security data transmission from one node to another should not be denied. This requirement is needed in order to trace the source of data. We consider three forms of data: one is forwarded from a node to another; the second is transmitted from a node to a cluster head or a sink; and on contrary, the third is delivered from a cluster head or a sink to a node.

(4) Authentication

A receiving sensor node must authenticate the identity of a sending sensor node. In case that the sender is a malicious node, the receiver can find it effectively. We consider three cases: the first is the authentication between two sensor nodes; the second is a cluster head or a sink should authenticate a sensor node; the third is on contrary, the cluster head or the sink should be authenticated by a sensor node exactly. Although public key cryptography is time-consuming, it is proved feasible to be used in WSNs [41], [42].

3.2 Criteria of Attack Detection

3.2.1 Traceability (Tr)

Traceability is preferred in attack detection. If a detection method can indicate the position of a malicious node clearly, we declare that this method has traceability. A good

detection method can not only detect an attack, but also accurately point out the position of the attack to allow further defence.

3.2.2 Accuracy (Ac)

Detection accuracy is the most important performance indicator of attack detection. Accuracy is used to show the ability of an attack detection method to distinguish malicious nodes and legitimate nodes. We use the following metrics to evaluate the accuracy of attack detection:

True Positive (TP): The number of nodes that is detected as malicious nodes when they are really malicious.

True Negative (TN): The number of nodes that is detected as legitimate nodes when they are indeed legitimate.

False Positive (FP): The number of nodes that is detected as malicious nodes but they are legitimate nodes contrarily.

False Negative (FN): The number of nodes that is detected as legitimate nodes but they are malicious nodes effectively.

We can use the True Positive Rate (TPR) and False Positive Rate (FPR) to measure the accuracy.

TPR: The ratio of TP to all malicious nodes. That is: *TPR=TP/(TP+FN).*

FPR: The ratio of FP to all legitimate nodes. That is: *FPR=FP/(FP+TN).*

If $TPR \geq 95\%$ and $FPR \leq 5\%$, we may declare that the underlying method is satisfactorily accurate.

3.2.3 False Tolerance (FT)

A detection method should be tolerant to the high ratio of malicious nodes to all sensor nodes. False tolerance is used to describe the adaptability of an attack detection method to a harsh environment. We define the false ratio as the ratio of malicious nodes to all sensor nodes. If a detection method can operate normally when the false ratio reaches a high value, we can say that the method has high false tolerance.

3.2.4 Applicability (Ap)

An attack method should be suitable to be applied in WSNs by considering its special constraints. Applicability refers to whether an attack method is applicable in the context of WSNs. It relates to two types of WSNs: Stationary Network (SN) and Mobile Network (MN). We should seriously take applicability into consideration since detection mechanisms are different from each other in different types of WSNs.

3.2.5 Scalability (Sc)

Scalability should be considered by an attack detection method in order to judge its possibility to be applied into a large-scale network. An application of WSN always consists of thousands and millions of sensor nodes in a large-scale scene. Some detection methods can only work well in the context of a small number of sensors. Their performance becomes unacceptable if the network scale is extended. Therefore, we need to consider the scalability of attack detection methods. If the accuracy, effectiveness and efficiency of an attack detection method do not obviously decrease with the increase of WSN node number, we can announce that it satisfies scalability.

4 Security Data Collection and Attack Detection

In this section, we summarize security data collection and attack detection methods of eleven mainstream attacks in WSNs. They are Jamming Attack (JA), Compromised Node Attack (CNA), Replication Node Attack (RNA), Denial-of-sleep Attack (DA), Sybil Attack (SA), Black Hole Attack (BHA), Gray Hole Attack (GHA), Wormhole Attack (WA), Sinkhole Attack (SHA), Hello Flooding Attack (HFA), and Flooding Attack (FA). We aim to summarize security data that are used to detect these attacks. Since there are few papers related to security data collection and attack detection methods of other types of attacks, we ignored them in this paper. In our survey, we refer to the papers about security data collection and attack detection from the following databases: IEEE Explorer Digital Library, ACM Digital Library, Elsevier ScienceDirect, Springer, Engineering Village (EI) and Web of Science (SCI). We survey the literature published in recent ten years using the keywords: attack (refers to a specific attack, e. g., wormhole attack) detection and WSN, or attack detection and WSN, etc. We review the literature based on the type of attacks, analyze the advantages and disadvantages of each detection method and evaluate the performance of security data collection based on the above proposed evaluation criteria. We sum up the performance of all reviewed works in Table 2 and the data of importance and magnitude that can be used to detect several attacks in Table 3, respectively. To the best of our knowledge, this is the first paper that gives an extensive overview and detailed performance analysis of mainstream attack detection methods in WSNs and summarizes the security data used in these methods towards WSN security measurement.

4.1 Attack Detection in Physical layer

4.1.1 Compromised Node Attack (CNA)

There are two types of methods [43], [44] to detect CNA. One is behavior-based method that can only detect misbehaviors (such as packet arrival rate, packet arrival time, node energy and node location), but cannot revoke the compromised node due to its nonzero FPR. The other is software attestation-based methods that check the insider code of nodes and can revoke malicious nodes, but it has high overhead.

In [44], [45], the network is divided into several zones (clusters). Adjacent zones would be expected to be loaded with similar communication overhead and computation cost. The central node of a zone evaluates trust levels of neighbor zones based on sequential hypotheses, and reports them to a sink. The sink will activate a software-based attestation system to detect each node in the zone with low trust value. Cryptographic algorithms were applied in these two works to ensure confidentiality, authentication and non-repudiation. Both works achieve good detection accuracy, and in [45], even though 34% of nodes are under attack, the detection rate can reach up to 99% and only 0.9% of false alarm is presented. All nodes in an untrustworthy zone are rechecked using software-based attestation. However, the authors did not consider DQ, DP,

integrity and DT. They did not clarify the communication overhead, either. Notably, there is no need to care about LP in these two works.

Thaile et al. [43] proposed a nodetrust-based method that a sink implements software attestation to check each untrustworthy node individually. The zone head evaluates trust values of each node based on packet arrival time. This method was applied in a stationary network. It can trace malicious nodes and meets EE since its communication overhead is only $\mathcal{O}(n)$. The authors did not consider DQ, integrity, DT and security properties, neither clarified accuracy, scalability and FT in their work. LP was not cared because it was not involved in this method.

In [46], a node collects packet dropping rate, packet sending rate and forwarding delay time to evaluate trust values of neighbor nodes. A node is regarded as a compromised node if the corresponding trust value is below a threshold. This scheme was applied in a stationary network. It can trace malicious nodes and meets EE since its communication overhead is only $\mathcal{O}(n)$. The authors considered DT in a way that a node assembles trust values of neighbors and filters the source nodes with deviated trust values. This scheme meets accuracy and FT because its testing result indicates that its detection rate is above 90% and its FPR is lower than 10%, even though 25% of sensors are compromised. A cryptographic technique was considered in this scheme. However, the authors did not consider DQ, DP and integrity. They did not clarify scalability, either.

4.1.2 Replication Node Attack (RNA)

RNA has been widely researched in previous work. A large number of detection methods have been presented to guard against this attack.

A Randomized, Efficient, and Distributed (RED) Protocol was proposed by Conti et al. [47] to detect replication node attacks in a stationry WSN. Every node knows its location using the method in [48] and keeps an ID-based pair-wise key [49]. Each node broadcasts a claim including ID and its location that is signed by its secret key. Neighbor nodes send the claim with probability p to a set of nodes that are selected pseudo-randomly for further collision detection. This protocol was applied in a stationary network. It can trace malicious nodes and is effective with low communication overhead of $\mathcal{O}(n)$. However, the authors did not consider DQ and integrity. On the other hand, this protocol does not satisfy with accuracy and scalability, because its detection probability is below 90% and will decrease as the number of nodes increases. Besides, LP and DP are exposed in this protocol. Notably, there is no need to consider DT herein because it is hard for malicious nodes to forge a claim of a normal node.

Xing et al. [50] proposed a fingerprint based real-time detection method in a stationary network. Each node reserves a codeword generated by a superimposed s-disjunct code [51] and computes its unique fingerprint based on its neighbors' codewords. The fingerprint is stored at each neighbor node and a sink and involved in every message sent to the sink. Neighbor nodes authenticate the authenticity of a node through comparing the consistency of the fingerprint in the message and the one in the local. Both neighbor nodes and the sink can detect replication nodes with this method. This method was applied in a stationary network. It can trace malicious nodes and it is effective because it generates redundant communication overhead of $\mathcal{O}(n)$ only in the process of fingerprint generation. Furthermore, it guarantees authentication of a node or the sink to a node, and ensures non-repudiation from a node to the sink or another node. However, the authors did not consider DQ and integrity. They did not clarify scalability and FT. Besides, there was no need to consider DT because it is hard for a malicious node to get fingerprints of normal nodes.

Area-Based Clustering Detection (ABCD) method was proposed by Naruephiphat et al. [52]. In this method, a node that has maximum neighbor nodes is selected as a central node. Then, the network is divided into several sub-areas with equal degree of angle. In each sub-area, a witness node is selected by using the method that is similar to choosing a central node. Every node sends a location claim with its node ID to the witness node in its area. If the witness node observes two messages with the same IDs but from different locations, it will send an alarm to all of nodes. Otherwise, it will send location claims to a sink to further detect. This method was applied in a stationary network. It can trace malicious nodes and it is effective because its communication overhead is $\mathcal{O}(n)$. Digital signature was applied to ensure authentication and non-repudiation. It meets accuracy and scalability because the detection rate is closed to 100% and nearly steady when the number of nodes changes. However, the authors did not consider DQ and integrity. LP and DP are exposed in this method. Notably, there was no need to consider DT because malicious nodes cannot forge IDs of normal nodes.

In [53], Dimitriou et al. proposed a detection method used in mobile WSNs and considered a situation that an adversary compromises a number of nodes to frame legitimate nodes. In this method, each of node generates a random nonce and exchanges it with each other when they meet for the first time. Later, when they meet again, they request each other for the previous value to verify authenticity. If a node cannot provide a genuine value, the other will keep the node ID in its quarantineList and send a claim to the sink. If the number of claims against a node ID received by the sink exceeds a threshold, which is above of the number of compromised identities, the sink will conclude this ID is a compromised ID and broadcast an alarm message to all nodes. This method satisfies the requirement of accuracy because it can always detect all replication nodes and has no false alarm if the threshold is set appropriately. Authentication and non-repudiation are guaranteed by applying digital signature. However, it does not satisfy scalability and EE since the communication overhead is $\mathcal{O}(n^2)$. In addition, the authors did not consider DQ, IoDS, DP, integrity, confidentiality and DT of claims sent from nodes to the sink. They did not clarify traceability and FT in the paper.

Recently, Ko et al. [54] suggested a Neighbor-Based Detection Scheme (NBDS). Every node keeps a table recording neighbor node information in this scheme, and when a

mobile node i wants to join a new community, its new neighbors would detect its validity through requesting its old neighbor nodes with a rejoining claim. The nodes that receive the rejoining claim will verify its validity and check if node i is still present in its neighborhoods by broadcasting an encrypted one-hop challenge message. Node i will reply an existence claim if it is still its neighborhood. Node i can be detected as a replicated node if both rejoining claim and existence claim are received by a previous neighbor node. This scheme was applied in a stationary network. Its communication overhead is $\mathcal{O}(m^2 \times n)$. Encryption and authentication techniques were applied comprehensively to provide confidentiality, integrity, authentication and non-repudiation. It meets accuracy since it can detect all replicated nodes if initial values of system parameters are set appropriately. However, it cannot ensure scalability and FT because its detection accuracy will decrease if the number of replicated nodes or false ratio increases. In addition, the authors did not consider DQ, IoDS, DP and DT of existing claims, and they did not clarify traceability. In another hand, Zhu et al. [55] declared that some forms of replicated node attacks would bypass this scheme and frame up legitimate nodes.

4.2 Attack Detection in Data Link Layer

People rarely focus on attack detection in the data link layer in WSNs. We only found few related papers about denial-of-sleep attack.

4.2.1 Denial-of-Sleep Attack (DA)

Researchers have proposed a number of Media Access Control (MAC) protocols to save energy and extend the life of sensor nodes [24], [22], [17]. For example, a sensor node switches between active mode and sleep mode in the duty-cycle based MAC protocols, such as B-MAC and X-MAC in which a sender node wakes up a receiver node by transmitting a specific preamble packet. Herein, we do not focus on these defense mechanisms in this paper since they do not relate to security data collection in these methods. Some detection methods related to security data collection are specified below.

In [27], Bhattasali et al. proposed a hierarchical framework based distributed collaborative mechanism for detecting denial-of-sleep attack. In this method, the authors divided a cluster into several sectors. In each sector, a sector-in-charge node is responsible for collecting sensing data from normal nodes and transmitting them to a sector monitor node that has the right to decide whether the data is valid or invalid and marks the data packets accordingly. A suspected node is detected if the number of packets from the same node exceeds a threshold limit within an interval or a packet is transmitted from a node in Sleep Mode. The monitor node then checks the residual energy of the suspected node and sends all packets to the cluster in which invalid data and suspected nodes are further analyzed to make a final decision. This mechanism was applied in a stationary network. It can trace malicious nodes and it is effective since its communication overhead is $\mathcal{O}(n)$. However, DQ, DP and some security properties were not considered in this mechanism. In addition, accuracy, FT and scalability were not clarified. Besides, there was no need to consider DT and LP in this mechanism.

Hsueh et al. proposed an authentication mechanism to identify the anti-nodes that force other legitimate nodes to be in active mode all the time [90]. A node that cannot respond with a correct ACK message for an encrypted challenge message sent by a cluster head is regarded as an anti-node. This mechanism runs in a stationary network. It can trace malicious nodes accurately. A hash chain is used for mutual authentication and session key agreement. Confidentiality and integrity are guaranteed by applying a hash function and a symmetric encryption algorithm. It meets EE with the communication overhead of $\mathcal{O}(n)$. However, the authors did not consider DQ, DP and non-repudiation. In addition, this paper does not provide experimental tests on attack detection, so that such criteria as accuracy, scalability and FT are hard to be judged. Besides, there is no need to consider DT in this mechanism.

4.3 Attack Detection in Network Layer

4.3.1 Sybil Attack (SA)

In [28], Newsome et al. put forward several schemes to detect the Sybil attack, mainly including a radio resource testing method. In this method, they assumed that a device is disabled to send and receive messages with multiple channels simultaneously. The detector sends some messages to its neighbors through different radio channels and waits for requests. Because the Sybil nodes have the same basic devices and cannot receive messages with multiple channels at the same time, they can be detected in the absence of acknowledge (ACK) messages. Its communication cost is non-negligible because it should run several rounds of iteration to achieve high accuracy. There are limited communication channels on the basis of IEEE 802.15.4 standard, which would reduce the accuracy of this method in a large-scale application as a node has many neighbors. A node would be identified as a Sybil node if it is on a sleep state or power depletion state. In addition, the authors did not consider data quality and many other performance objectives. Besides, there is no need to consider DT in this scheme.

Murat and Youngwhan [60] proposed a lightweight method for Sybil node detection in WSNs based on RSSI. There is a theory that every node can expose its location if at least four nodes monitor the ratio signal simultaneously [57]. In this method, four sensor nodes ascertain the location of the detected node through RSSI cooperatively. If the node has the same location but different sending-IDs through multiple detections, we can affirm that it is a Sybil node. This method was applied in a stationary network. It can trace malicious nodes and it is efficient because its communication complexity is $\mathcal{O}$(n). However, other criteria were not considered in this work.

Then, Wang et al. improved the aforementioned method in [61]. They thought over Rayleigh fading in a practical wireless channel and combined RSSI with various parameters such as position and power value. They established a system that monitoring nodes can send alarm data after detecting abnormity and it is worthwhile to increase about 2 percent of communication consumption. The proposed

system runs in a stationary network. It can trace malicious nodes and it is efficient because its communication complexity is $\mathcal{O}$(n). It can satisfy DQ since the effect of environment on security data was considered. However, the accuracy of attack detection is below 95%. The authors did not consider DT, privacy, scalability and some security properties. FT was not clarified, either.

Clock skew is a unique characteristic of a sensor node and different sensor nodes have constant and different clock skews. Huang et al. [62] made use of the Flooding Time Synchronization Protocol (FTSP) to collect clock skew information of neighbor nodes. If nodes with different IDs have the same clock skew, then we can allege that the whole network is under Sybil attack. For identifying all neighbor nodes, a node should keep each neighbor's minimum clock skew, maximum clock skew and average clock skew with little computation and memory. This protocol was applied in a stationary network. It can trace malicious nodes and it is efficient because its communication consumption linearly increases corresponding to the number of nodes and neighbor nodes. It satisfies with accuracy since it can detect all malicious nodes and its FPR is equal to 0.000125. There is no need to consider DT because malicious nodes cannot forge clock skew and ID of a normal node. Other quality properties were not considered in this protocol. We can also use this protocol to detect replication node attack since replicated nodes have different clock skews although holding the same ID.

4.3.2 Black Hole Attack (BHA)

In general, a node collects and analyzes the Packet Delivery Ratio (PDR) value from neighborhoods to detect BHA. If the PDR is zero, the detected neighbor node is suspected to be a malicious node. However, this method is not so accurate because the PDR of a node is almost zero when it suffers from congestion or jamming attack.

Prachi et al. [63] made use of PDR and time delay to detect BHA in a cluster based WSN. If the PDR of a node is always equal to zero for a specific period, the node is confirmed to be a black hole node. The authors proposed a defense mechanism by using two cluster heads in a cluster. Every activated cluster head stores a member list in its cluster and removes malicious member IDs. If the cluster head is a black hole node, the sink would remove it and activate another cluster head. This method runs in a stationary network. It can trace malicious nodes and it is efficient because its communication overhead is $\mathcal{O}(n)$. FT, accuracy and scalability were not specified and the specific threshold for judging whether a node is a black hole node is hard to ascertain in this method. In addition, the authors did not consider DQ, DT, DP, integrity and security properties.

In [64], Alattas presented a method for detecting BHA in a stationary network using several sinks and a check agent, which is a self-controlling software programme. Each node keeps a list of neighbor nodes. In general, the network works in the state of a nearest sink routing algorithm and the check agent visits every node randomly to check the receiving packet frequency for each neighbor node. If the frequency decreaces to zero, the agent will activate a multiple sink routing algorithm to check whether the neighbor node is a black hole node continually. This method was applied in a stationary network. It can trace malicious nodes and it is efficient because its communication overhead is $\mathcal{O}(n)$. The authors did not clarify accuracy and FT because they did not consider FPR in their work. In addition, DQ, DT, DP, integrity and security properties were not considered. This method does not match scalability since its detection accuracy decreases when the number of nodes increases.

Motamedi and Nasser [65] developed a method using Unmanned Aerial Vehicles (UAV) to take the place of mobile agents and applied a dynamic threshold to determine whether the detected node is a black hole node. This method was applied in a stationary network. It can trace malicious nodes with negligible communication overhead. However, the authors did not clarify accuracy and FT because they did not consider FPR. The method is not scalable since its detection accuracy decreases linearly with the increase of the scale of WSN. It does not consider the security properties, DQ, DT, DP and integrity.

Roy et al. [2] utilize multiple security data to evaluate trust value of a sensor node. If the trust value is below a defined threshold, this network is under BHA or SHA based on different abnormal data. This method can be used in a stationary network. It can trace malicious nodes and it is efficient with communication overhead of $\mathcal{O}(n)$. The authors considered DT in such a way that a node assembles trust values from neighbors. However, they omitted accuracy, FT and scalability, as well as other criteria.

Prathapani et al. [66] proposed a method by using an intelligent honeypot agent. Different from above mentioned methods, the agent sends an exclusive RREQ message to a "testee" with a randomly known destination. If the "testee" produces a RREP message and declares it is the nearest route to the destination, the honeypot agent sends a normal packet to the destination through the "testee" and asks the destination node whether it has received the packet. This method runs in a stationary network. It can trace malicious nodes and it is efficient with communication overhead of $\mathcal{O}(n)$ It meets the requirements on accuracy and FT since the TPR of this method can be up to 100% when 5% of network is under attack and the accuracy is also very good when 20% of network is under attack. However, the authors did not clarify scalability and consider other criteria.

4.3.3 Gray Hole Attack (GHA)

It is more difficult to detect GHA compared with BHA because malicious behaviors in GHA are similar to normal packet drops.

Park et al. [67] proposed an energy-efficient method to detect GHA. A sink stores the average communication time of every node. If the actual communication delay of a node exceeds a threshold, the sink will activate the detection mechanism and transmit a Retransmission request message to the source node. Many checkpoint nodes are deployed in a path in this method, which send acknowledge-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2883403, IEEE Internet of Things Journal

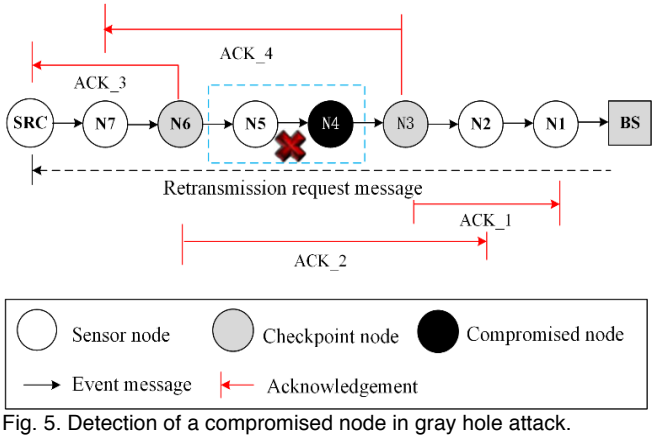

Fig. 5. Detection of a compromised node in gray hole attack.

ment (ACK) messages to the sink after they receive the Retransmission request message and send ACK messages to the source node after they receive the Retransmission message as illustrated in Fig. 5. Then checkpoint nodes can detect a compromised node based on ACK messages. This method runs in a stationary network and it can trace malicious nodes. It is energy-efficient since it activates the detection mechanism only when the sink discovers a suspicious node. Its maximum communication overhead is $\mathcal{O}(k)$, thus efficient. In addition, it is accurate becausee its detection TPR is 97% and FPR is below 5%. Specially, its TPR can be up to about 88% when 25% of nodes are compromised. However, the authors did not consider other criteria.

In [69], Li et al. presented a method that a cluster head runs Sequential Mesh Test after receiving a packet dropping report from a node. This method can be also used to detect BHA, but it cannot stop a malicious node from sending a mendacious packet dropping report to a cluster for vilifying a normal node. The report is encrypted with a symmetric encryption algorithm to guarantee its confidentiality. This method runs in a stationary network and it can trace malicious nodes. It is efficient because the detection method is activated based on demand and only needs a few samples to run the test, and its maximum communication overhead is $\mathcal{O}(m \times n)$. It satisfies FT because its accuracy can reach 90% even when more than 70% of nodes are compromised. There is no need to consider DT and LP. However, this method does not meet other criteria.

Ren et al. [72] proposed a detection method based on a trust evaluation mechanism. A node monitors forwarding traffic of its neighbor nodes and evaluates trust levels based on the deviation between average packet dropping ratio and actual packet dropping ratio as well as trust reports from neighbor nodes of the detected node. They set up different thresholds to mitigate the influence of an environment and consider data quality by weighting the trust reports from neighbor nodes. A sink uses the average trust value and the standard deviation of trust levels to alleviate the influence of malicious nodes. It can also be used to detect BHA. This method runs in a stationary network to trace malicious nodes. It is energy efficienct since the communication overhead is $\mathcal{O}(m \times n)$. This method takes advantage of cryptographic techniques to guarantee confidentiality and authentication against adversaries. Moreover, it can always achieve more than 95% of TPR if less than 50% of nodes are compromised in the network, thus this method satisfies accuracy and FT. However, the authors did not clarify scalability and non-repudiation, and they did not consider other criteria.

In [71], Dharini et al. proposed an energy consumption-based method to detect flooding attack and gray hole attack in a stationary network. Through simulation, flooding attack consumes the maximum energy of a node, while gray hole attack consumes the minimum energy of a node. A cluster head dynamically predicts energy consumption of a sensor node in the next interval. If the predicted energy consumption is more than actual energy consumption, the node will be regarded as suffering flooding attack. On contrary, if the predicted energy consumption is less than actual energy consumption, the node will be considered as a malicious node launching gray hole attack. This method detects flooding attack and gray hole attack with high effectiveness and efficiency since extra requested traffic and calculation are very limited. What's more, the cluster head can trace a malicious node and isolate it from the network. DT and LP are unnecessary to be considered in this method. Besides, DP, DQ and security properties were not considered. Accuracy, FT and scalability were also omitted.

4.3.4 *Wormhole Attack (WA)*

The detection method proposed by Zaw et al. [73] is based on the assumption that the number of adversaries' neighbor nodes are more than those of normal nodes, and Round Trip Time (RRT) of RREQ sent by a source node and corresponding RREP replied by a destination node in AODV routing protocol is raised if an adversary exists in the WSN. If RRT and the number of neighbor nodes of node A and node B are considerably higher than a threshold, we can assume that A and B are wormhole nodes. This method was applied in a stationary network and can trace malicious nodes. It does not request any extra hardware and communication overhead to detect wormhole attacks. Its computation requirement is small. However, it does not meet accuracy because its detection accuracy decreases sharply when two wormhole nodes are less than 5 hops apart. In addition, Zaw et al. did not consider security properties and DQ in actual situations where radio signals are susceptible. Besides, the authors did not consider DT because the number of neighbor nodes can be forged by Sybil attack. In [74], Subha and Sankar developed the method that uses a modified ElGamal signature scheme to guarantee authentication and non-repudiation.

Luo et al. [75] presented a real-time and passive wormhole detection method, named Pworm, which can detect and locate malicious nodes in a stationary network based on the insight that the path length would reduce and the traffic flow would increase around wormhole nodes. This method runs in a stationary network to trace malicious nodes. The authors considered EE since the method only introduces a little communication overhead. The method can detect more than 95% of malicious nodes by applying a suitable threshold, but FPR is omitted in this work, thus accuracy, FT and scalability were not clarified. It makes use

of a message authentication code to protect the integrity of messages. DQ, DT and other criteria were not considered in this work.

A two-phase detection method in mobile network was proposed in [76]. A node detects the rate of change of neighbor (RCN) nodes at real time. If it locates at an interval between lower and upper threshold, the method will activate the second phase that detects the alternate path lengths of nodes in a suspected set. This method can be applied in a mobile network to trace malicious nodes accurately. It is efficient with suitable communication overhead of $\mathcal{O}(m \times n)$. However, it does not meet accuracy, because TPR is below 95%. In addition, FT and scalability were not clarified. The authors did not consider other criteria.

In [77], Garcia-Otero and Poblacion-Hernandez presented a detection approach based on a special range-free localization method. The authors proposed two detection strategies by using at least four anchor nodes to collect RSSI and fixed locations of normal nodes in a stationary network. This approach can trace malicious nodes accurately. The authors considered shadowing effects, to which detection accuracy is sensitive. Its TPR increases linearly along with FPR, thus its accuracy is not so satisfied. In the process of data communications, integrity and confidentiality are ensured with a cryptographic algorithm. This approach can meet EE due to suitable communication overhead of $\mathcal{O}(n)$. Other criteria were not considered in this work.

4.3.5 Sinkhole Attack (SHA)

Guerroumi et al. [78] proposed a detection method in WSNs with a mobile sink. The network is modeled as a virtual grid comprised of several cells. The sink moves periodically or randomly to a cell with the highest dissemination rate to reduce end-to-end delay, throughput and power consumption in a stationary network. But it is prone to be subjected to sinkhole attack, which draws a lot of traffic with false topological and positional information. The authors utilized advertisement messages including the coordinates and the detection rate of the destination cell sent from the sink to all cell leaders to distinguish between the valid and false sinks. This method can be applied in a stationary network. Its detection rate is high and keeps stable as the number of nodes increases. DT and LP are unnecessary to be considered in this method. However, it wastes lots of energy to update routing messages and fix position of each cell using GPS [77]. FT and scalability were not clarified, and other criteria were not considered, either.

In [79], Salehi et al. presented a method in a stationary network. The sink checks the consistency of data to find a group of suspicious nodes, and then figures out a specific intruder by analyzing network traffic. This method can be applied in a stationary network to trace malicious nodes. It is efficient since most computation runs in the sink and its communication overhead is $\mathcal{O}(n)$. It meets the requirements of accuracy and FT because its success rate is nearly 100% when there are few collusive nodes and is still 80% even when the rate of collusive nodes is up to 50%. The authors did not consider other criteria and a malicious node can slander normal nodes optionally by sending numerous false data packets.

Chen et al. [80] proposed a change-point detection method to monitor the consistency of CPU usage in each node. Because the malicious node would draw lots of packets destined to the sink, the CPU usage of it would increase obviously during the period of processing so many packets. They used Girshick Rubin Shyriaev (GRSh) method [81] to discriminate a legitimate node loaded a high burden for a short time from a malicious node. This method can trace malicious node accurately. It is efficient because its communication overhead increases linearly with the number of nodes. The authors considered the effect of environment on security data; thus, it meets DQ. In theory, this method satisfies accuracy and FT, which, however, were not verified in experiments. Other criteria were not considered in this work.

Sharmila et al. [82] suggested a method in a stationary network that compares the consistency of a digest sent to the sink via an old trustable path with the shorter one through a new node. This method can be applied in a stationary network to trace malicious nodes. It is efficient since its communication overhead is $\mathcal{O}(n)$. It meets accuracy and FT because it has high success rate, which is still about 80% when malicious nodes occupy half of the network. FPR keeps 0 until the ratio of malicious nods gets up to 30%. However, the authors did not clarify scalability and other criteria were not considered, either. Notably, the detection result is not trustworthy if the new node is under jamming attack.

Tumrongwittayapak et al. [83] proposed a method based on the assumption that if the routing of a static node to the sink is changed, then a sinkhole attack is present. They used four extra monitor (EM) nodes to determine the position of all sensor nodes that send data (Node ID, Next Hop ID, RSSI value) to the RSSI Based Sinkhole Detector (RBSD) resided in the sink. If the RSSI value is constant but Next Hop ID of a node is different from the previous one, then a sinkhole attack will occur at the nearest node to the sink in the routing since the malicious node has only one-hop route to the sink. This method can be applied in a stationary network to trace malicious nodes. It is lightweight since it only introduces communication overhead of $\mathcal{O}(n)$. It meets accuracy and FT because the detection rate is above 95% although the ratio of malicious nodes increases from 0 to 20%. But the authors did not consider the impact of WSN environment. They did not clarify scalability and other criteria. Notably, this method did not meet DT because topology can be changed due to node failure. What's more, this method did not distinguish sinkhole attack from wormhole attack that can also change the routing from a node to the sink.

In addition, Dallas et al. [84] suggested an approach to detect hop-count values of a node residing in route advertisements. It is an indication of sinkhole attack if the hop-count changes significantly. This Anomaly Detection System (ADS) only can be deployed in a stationary network. It can achieve 96% of TPR and 5% of FPR with only one single ADS. The detection rate will get up to 100% with 5

ADSs. This approach does not request any extra communication overhead. But it cannot discover the specific location of a malicious node. The authors did not consider other criteria (such as scalability and security properties). This method has the same problem as [83] since node failure and wormhole attack can change hop-count values significantly.

4.3.6 Hello Flooding Attack (HFA)

Some cryptography-based approaches [85], [86], [87] were proposed to defend HFA. We only consider non-cryptographic approaches because it is difficult to conclude the security data used in the existing cryptography-based methods.

In [88], each node sets a threshold for RSSI. If received RSSI of a node is equal to fixed signal strength in its radio range, the node treats the sender as a friend. Otherwise, it treats the sender as a stranger if received RSSI is more than fixed signal strength. When RSSI is similar to the threshold but not the same, the node sends a test message to the sender. If it receives a reply within a specified time, it classifies the sender as a friend, otherwise a stranger. In [89], Magotra et al. improved the aforementioned method. The test message and its corresponding response are replaced by coordinate information of the sender node. Only the nodes whose RSSI and distance are both within the threshold are considered as friends. Above methods can be applied in a stationary network. They can trace malicious nodes accurately and meet EE with the communication overhead of $\mathcal{O}(n)$. The authors did not clarify accuracy, FT and scalability. DT and LP are unnecessary to be considered. Besides, other criteria were not considered.

4.4 Attack Detection in Transport Layer

Few studies were found to detect attacks occurring in the transport layer. Existing work mainly focuses on flooding attack detection.

4.4.1 Flooding Attack (FA)

As mentioned before, Dharini et al. proposed an energy consumption method to detect flooding attack and gray hole attack accurately and effectively [71]. The performance analysis is the same as before.

In [91], Rolla et al. proposed a dynamic time-based forwarding window technique to detect and prevent flooding attack in a stationary network. The authors divided all neighbor nodes of a source node into two parts. The source node transmits RREQ messages to its first part of nodes and informs the second half part of nodes the number of neighbor nodes and the time at which RREQ messages were initiated in order to calculate the dynamic time called forwarding window. If any malicious node is located in the communication range of the second part of nodes, it will flood the network with RREQ messages. The second part of nodes will detect the malicious node whose duration of sending packets is more than the forwarding window and inform the malicious node ID to other nodes. This technique can be applied in a stationary network to trace malicious nodes. It is lightweight since its communication overhead is $\mathcal{O}(m \times n)$. However, privacy, DQ, DT and security properties were not considered and accuracy, FT and scalability were omitted in this study.

4.5 Attack Detection across Multiple Layers

4.5.1 Jamming Attack (JA)

We do not distinguish basic jamming attack (BJA) from intelligent jamming attack (IJA) because most detection schemes can detect both attacks. Jamming attack has a significant influence on packet dropping ratio, packet delivery ratio, energy consumption and other performance indicators, so that we can use these indicators to detect jamming attacks.

Xu et al. [56] applied three basic statistics (RSSI, carrier sensing time and PDR respectively to evaluate whether the channel is under a jamming attack. They distinguished normal traffic from most of jamming attacks except for reactive jammer based on RSSI through a large number of simulation experiments. Carrier sensing time can be used to effectively detect constant jammers and deceptive jammers, and it can differentiate congestion from jamming. But using this data becomes invalid for finding random jammers and reactive jammers. Finally, PDR is an effective statistic to discriminate all jammer models from normal traffic and congested scene, which is also utilized in [58], but it is ineffective for other network dynamics (such as power exhaustion) because these situations result in extremely low PDR just like a jammer does. All of the above three schemes are effective and efficient based on the communication overhead of $\mathcal{O}(n)$.

In [19], Xu et al. specified an advanced method by using a mixed scheme. They used RSSI and PDR at the same time to identify a jamming attack. This method can verify all types of jammers and further distinguish the jamming attack from network dynamics. Only high signal strength with low PDR is the symbol of a jammed area. This method can be applied in a stationary network. It is efficient because of communication overhead $\mathcal{O}(n)$. But such criteria as DQ, confidentiality, authentication and integrity were not considered, and accuracy, FT and scalability were not clarified in this study. Besides, DT and LP are unnecessary to be considered. The authors presented two countermeasures against jamming attacks named channel surfing and spatial retreats. The former utilizes a coordinated channel switching and spectral multiplexing technique to prevent jamming attacks. The latter is applied into a mobile network where all of victim nodes can get away from an interference area.

Manju et al. [59] also took RSSI and PDR into consideration to detect a jammer node because it prevents communications between two normal nodes and may impact the channel quality and reduce the PDR. A node with the maximum Residual Energy (RE) is elected to be a monitoring node and monitors abnormal PDR and RSSI of its neighbor nodes periodically. But the authors did not consider the situation that a malicious node serves as a monitoring node and it always happens because a malicious node often has the maximum RE. This method can be applied in a stationary network to trace malicious nodes. It is efficient due to communication overhead of $\mathcal{O}(n)$. However, the authors did not clarify accuracy, FT and scalability of the proposed

method and did not consider DQ, DT and security, either.

TABLE 2.

SECURITY DATA AND PERFORMANCE EVALUATION OF ATTACK DETECTION METHODS IN WSNS

Layer	Attack	RE	Collected Security Data	Criteria of Security Data Collection													Criteria of Attack Detection				
				Data Quality	DT	EE	Privacy		Integrity	Conf	Non-repudiation			Authentication			Traceability	Accuracy	FT	Applicability	Scalability
							LP	DP			NN2C	NN2N	NC2N	AC2N	AN2N	AN2C					
PL	CNA	[44], [45]	Inconsistent data, Trust values.	×	×	*	*	×	×	√	√	√	×	√	√	×	√	√	√	SN	*
		[43]	Packet arrival time, Trust values.	×	×	√	*	×	×	×	×	×	×	×	×	×	√	*	*	SN	*
		[46]	PDR, Packet sending rate, Forwarding delay time, Trust values.	×	√	√	*	×	×	√	√	√	×	√	√	×	√	√	√	SN	×
	RNA	[47]	A claim: ID and location	×	*	√	×	×	×	√	√	√	×	√	√	×	√	×	×	SN	×
		[50]	Fingerprint	×	*	√	*	×	×	×	√	√	×	√	√	×	√	√	*	SN	*
		[52]	Location claim	×	*	√	×	×	×	×	√	√	×	√	√	×	√	√	*	SN	√
		[53]	A random nonce	×	×	×	*	×	×	×	√	√	×	√	√	×	*	√	*	MN	×
		[54]	Rejoining claims, Existence claims.	×	×	×	*	×	√	√	√	√	×	√	√	×	*	√	×	MN	*
DLL	DA	[27]	The number of packets during an interval, Abnormal packets, Residual energy.	×	*	√	*	×	×	×	×	×	×	×	×	×	√	*	*	SN	*
		[90]	ACK packets	×	*	√	*	×	√	√	×	×	×	√	√	√	√	*	*	SN	*
NL	SA	[28]	ACK packets	×	*	×	*	×	×	×	×	×	×	×	×	×	*	√	*	*	×
		[60]	RSSI, Sender-ID.	×	×	√	×	×	×	×	×	×	×	×	×	×	√	*	*	SN	×
		[61]	RSSI, Sender-ID, Position, Power values.	√	×	√	×	×	×	×	×	×	×	×	×	×	√	√	*	SN	×
		[62]	Clock skew, Sender-ID.	×	*	√	*	×	×	×	×	×	×	×	×	×	√	√	*	SN	×
	BHA	[63]	PDR, Carrier sensing time.	×	×	√	*	×	×	×	×	×	×	×	×	×	√	*	*	SN	*
		[64]	Received packet frequency	×	×	√	*	×	×	×	×	×	×	×	×	×	√	*	*	SN	×
		[65]	Received packet frequency	×	×	√	*	×	×	×	×	×	×	×	×	×	√	*	*	SN	×
		[2]	PDR, Number of hops for received packets	×	√	√	*	×	×	×	×	×	×	×	×	×	√	√	*	SN	*
		[66]	RREP, Query reply packet.	×	×	√	*	×	×	×	×	×	×	×	×	×	√	√	√	SN	*
		[67]	Communication delay, ACK packets.	×	×	√	*	×	×	×	×	×	×	×	×	×	√	√	√	SN	*
		[69]	PDR, Data packets.	×	*	√	*	×	×	√	×	×	×	×	×	×	√	√	√	SN	×
		[72]	PDR, Trust values.	√	×	√	*	×	×	√	*	*	×	√	√	×	√	√	√	SN	*
	GHA	[67]	ACK packets	×	×	√	*	×	×	×	×	×	×	×	×	×	√	√	√	SN	*
		[69]	Packet dropping reports	×	*	√	*	×	×	√	×	×	×	×	×	×	√	×	√	SN	×
		[72]	PDR, Trust evaluation levels.	√	×	√	*	×	×	√	*	*	×	√	√	×	√	√	√	SN	*
		[71]	Initial energy, Residual energy.	×	*	√	*	×	×	×	×	×	×	×	×	×	√	*	*	SN	*
	WA	[73]	RTT, The number of neighbor nodes.	×	×	√	*	×	×	×	×	×	×	×	×	×	√	×	*	SN	*
		[74]	RTT, The number of neighbor nodes.	×	×	√	*	×	×	×	√	×	×	√	×	×	√	×	*	SN	*
		[75]	Path lengths, Traffic flow.	×	×	√	*	×	√	×	×	×	×	×	×	×	√	*	*	SN	*

		[76]	RCN, The alternative path lengths.	×	×	×	*	×	×	×	×	×	×	×	×	×	√	*	*	MN	*
		[77]	RSSI	√	×	√	×	×	√	√	×	×	×	×	×	×	√	×	*	SN	*
	SHA	[2]	PDR, Number of hops for received packets	×	√	√	*	×	×	×	×	×	×	×	×	×	√	√	*	SN	*
		[78]	Advertisement messages	×	*	×	*	×	×	×	×	×	×	×	×	×	×	√	*	SN	*
		[79]	Inconsistent data, Network traffic.	×	×	√	*	×	×	×	×	×	×	×	×	×	√	√	√	SN	*
		[80]	CPU usage information	√	×	√	*	×	×	×	×	×	×	×	×	×	√	*	*	*	×
		[82]	Message digest	×	×	√	*	×	×	×	×	×	×	×	×	×	√	√	√	SN	*
		[83]	Data (Node ID, Next Hop ID, RSSI value)	×	×	√	×	×	×	×	×	×	×	×	×	×	√	√	√	SN	*
		[84]	Hop-count values	×	×	√	*	×	×	×	×	×	×	×	×	×	×	√	*	SN	×
	HFA	[88]	RSSI	×	*	√	*	×	×	×	×	×	×	×	×	×	√	*	*	SN	*
		[89]	RSSI, Coordinate information	×	*	√	*	×	×	×	×	×	×	×	×	×	√	*	*	SN	*
TL	FA	[71]	Initial energy, Residual energy.	×	*	√	*	×	×	×	×	×	×	×	×	×	√	*	*	SN	*
		[91]	Duration of sending RREQ messages	×	×	√	*	×	×	×	×	×	×	×	×	×	√	*	*	SN	*
ML	JA	[56]	RSSI / Carrier sensing time	×	*	√	× / *	× / ×	×	×	×	×	×	×	×	×	×	*	*	SN	×
		[56], [58]	PDR	×	×	√	*	×	×	×	×	×	×	×	×	×	×	*	*	SN	×
		[19]	RSSI, PDR.	×	*	√	*	×	×	×	×	×	×	×	×	×	×	*	*	SN	*
		[59]	RSSI, PDR.	×	×	√	×	×	×	×	×	×	×	×	×	×	√	*	*	MN	*

RE: References
FT: False Tolerance
DT: Data Trustworthiness
Confi: Confidentiality
NN2C: Non-repudiation of data from a node to a cluster head or a sink
NN2N: Non-repudiation of data from a node to another node
NC2N: Non-repudiation of data from a cluster head or a sink to a node
AC2N: Authentication of a cluster head or a sink towards a node
AN2N: Authentication of a node towards another
AN2C: Authentication of a node towards a cluster head or a sink
PL: Physical Layer
DLL: Data Link Layer
NL: Network layer
TL: Transport Layer
ML: Multiple Layers
√ denotes that the method satisfies the criterion.
× denotes that the method does not match the criterion.
** denotes that the method does not care about the criterion or whether the method meets the criterion or not is not clarified.*

4.6 Summary

4.6.1 Security Data and Performance of Attack Detection

We summarize security data and performance evaluation result of all reviewed detection methods in Table 2.

We summarize the important and typical security data that can detect multiple attacks in Table 3. We first observe that security data RSSI can be used to detect 5 types of attacks simultaneously: JA, SA, WA, SHA and HFA. Second, we can use PDR to detect 4 types of attacks: CNA, JA, BHA and GHA. ACK packets are also used in the detection for 4 types of attacks: SA, BHA, GHA and DA. Next, trust values are related to three types of attacks: CNA, BHA and GHA. We can apply initial energy and residual to detect GHA, HFA and FA. Finally, location claims and carrier sensing time can be used to detect two types of attacks.

Furthermore, from the above review, we find that most of detection methods are applied to a stationary network, while only few of methods are proposed with regard to mobile networks. Traceability as well as effectiveness and efficiency are considered adequately since many existing methods can point out the position of the attack accurately and take power consumption into account. But few methods consider data quality, scalability and data trustworthiness when detecting attacks. Accuracy is a fundamental criterion so that most of methods meet it. What's more, about half of methods achieve high false tolerance ratio. However, security properties are seldom considered in all

TABLE 3
IMPORTANT AND TYPICAL SECURITY DATA TO DETECT MULTIPLE ATTACKS

Security data	The number of detected attacks	Detected attacks
RSSI	5	JA, SA, WA, SHA, HFA
PDR	4	CNA, JA, BHA, GHA
ACK packets	4	SA, BHA, GHA, DA
Trust values	3	CNA, BHA, GHA
Initial energy and residual energy	3	GHA, HFA, FL
Location claims	2	RNA, SA
Carrier sensing time	2	JA, BHA

methods to guarantee confidentiality, integiry, authentication and non-repudiation of security data in the process of data transmission. Especially, no methods think over privacy. It is still an open issue right now.

4.6.2 Data Collection and Detection of Synthesized Attacks

Park et al. [67] proposed an energy-efficient method that can detect BHA or GHA. If a checkpoint node cannot reply ACK message accurately, we think this network is under BHA or GHA. This method can be applied in a stationary network to trace malicious nodes. It saves energy since it activates the detection mechanism only when the sink discovers a suspicious node, and its maximum communication overhead is $\mathcal{O}(k)$. In addition, it meets accuracy because its TPR is 97% and FPR is below 5%. Specially, its TPR can be up to about 88% when 25% of nodes are compromised. However, the authors did not consider other criteria.

Through a number of experiments, Dharini et al. [71] discovered that among DoS attacks, gray hole consumes the minimal amount of energy, while flooding attack consumes the maximal amount of energy. Ultimately, they utilized energy consumption to distinguish between GHA and FA. This method detects flooding attack and gray hole attack with high effectiveness and efficiency, since extra requested traffic and computation of this method are very limited. What's more, a cluster head can trace a malicious node and isolate it from the network. DT and LP are unnecessary to be considered in this method. Besides, DP, DQ and security properties were not considered. Accuracy, FT and scalability were also omitted.

In [69], Li et al. presented a method that a sensor node can monitor its neighbor nodes retransmission traffic with a Watchdog [70] or an ACK message. This method can detect BHA and GHA according to the amount of retransmission traffic. Data is encrypted with a symmetric encryption algorithm to guarantee its confidentiality. This method can be applied in a stationary network to trace malicious nodes. It is efficient because the detection method is activated based on demand. Its maximum communication overhead is $\mathcal{O}(m \times n)$. It meets FT because its accuracy can reach 90% even when more than 70% of nodes are compromised. There is no need to consider DT and LP. However, this method does not meet other criteria.

Ren et al. [72] proposed a method that can detect GHA or BHA based on a trust evaluation mechanism. A node evaluates the trust value of a neighbor node based on the deviation between average packet dropping ratio and actual packet dropping ratio as well as trust reports from neighbor nodes. When the average trust value of a node is below a defined threshold, we think this node is under GHA or BHA. This method can be applied in a stationary network for tracing malicious nodes. It is energy efficient since its communication overhead is $\mathcal{O}(m \times n)$. This method takes advantage of cryptographic techniques to guarantee confidentiality and authentication against adversaries. Moreover, it can always achieve more than 95% of TPR if less than 50% of nodes are compromised in the network, thus this method satisfies accuracy and FT. However, the authors did not clarify scalability and non-repudiation, and did not consider other criteria.

Roy et al. [2] proposed a scheme that uses Dynamic Trust Management system (DTMS) to counter BHA and SHA simultaneously. It utilizes multiple security data to evaluate the trust value of a sensor node. If the trust value is below a specific threshold, we declare that this network is under BHA or SHA based on different abnormal data. This scheme can be applied in a stationary network to trace malicious nodes. It is efficient with communication overhead of $\mathcal{O}(n)$. The authors considered DT in a way that a node assembles trust values from neighbors. However, the authors omitted accuracy, FT and scalability, and did not consider other criteria.

Other schemes [56], [58], [59], [19] use multiple security data such as RSSI, carrier sensing time, PDR to jointly detect basic jamming attack and intelligent jamming attack. When

TABLE 4
Security Data and Performance Evaluation of Attack Detection Methods for Synthesized Attacks in WSNs

RE	Attacks	Collected Data	Criteria of Security Data Collection													Criteria of Attack Detection				
			Data Quality	DT	EE	Privacy		Integrity	Conf	Non-repudiation			Authentication			Traceability	Accuracy	FT	Applicability	Scalability
						LP	DP			NN 2C	NN 2N	NC 2N	AC 2N	AN 2N	AN 2C					
[67]	BHA, GHA	Communication delay, ACK packets.	×	×	√	*	×	×	×	×	×	×	×	×	×	√	√	√	SN	*
[71]	GHA, FA	Initial energy, Residual energy.	*	*	√	*	×	×	×	×	×	×	×	×	×	√	√	*	SN	*
[69]	BHA, GHA	PDR, Data packets.	×	*	√	*	×	×	√	×	×	×	×	×	×	√	√	√	SN	×
[72]	BHA, GHA	PDR, Trust values.	√	×	√	*	×	×	√	*	*	×	√	√	×	√	√	√	SN	*

[2]	BHA, SHA	PDR, Number of hops for received packets	×	√	√	*	×	×	×	×	×	×	×	×	√	√	*	SN	*
[56]	BJA, IJA	RSSI	×	*	√	×	×	×	×	×	×	×	×	×	×	*	*	SN	×
		Carrier sensing time	×	*	√	*	×	×	×	×	×	×	×	×	×	*	*	SN	×
		PDR	×	×	√	*	×	×	×	×	×	×	×	×	×	*	*	SN	×
[58]		PDR	×	×	√	*	×	×	×	×	×	×	×	×	×	*	*	SN	×
[19]		RSSI, PDR.	×	*	√	×	×	×	×	×	×	×	×	×	×	*	*	SN	*
[59]		RSSI, PDR.	×	×	√	×	×	×	×	×	×	×	×	×	√	*	*	MN	*

the value of security data exceeds defined threshold, we think this network is under jamming attack. These schemes are efficient because of communication overhead $\mathcal{O}(n)$. They can be applied in a stationary network, but cannot trace malicious nodes accurately except for [59]. There was no need to consider DT in [19] and the first two schemes in [56]. Other criteria such as DQ, confidentiality, authentication and integrity were not considered, and accuracy, FT and scalability were not clarified in these schemes.

For easy conclusion, we summarize the performance of the above reviewed literature methods in Table. 4. The security-related data collected in each method are also summarized.

5. Open Issues and Future Research Directions

Based on the analysis of existing attack detection methods, we come across a number of open issues on security data collection and security measurement as outlined in Section 5.1. Furthermore, we attempt to propose a list of future research directions in Section 5.2.

5.1 Open Issues

We propose a number of open issues based on the above comprehensive review and performance analysis in terms of security data collection and security measurement in WSNs.

First, an attack detection and security measurement method that is adaptive to the trust of the sink is still missed in the literature. All of the existing centralized methods were proposed based on an assumption that the sink is a completely trusted equipment, which is never attacked and destroyed in all scenes. In practice, however, a mighty adversary can intrude it, which has occurred in reality. In general, the central facilities are the first to bear the brunt in a war and easily destroyed in a natural disaster (e.g., an earthquake and a flood). Thus, the attack detection and security measurement method that is adaptive to the trustworthiness of the sink should be studied.

Second, the literature lacks a holistic method that can detect most of mainstream attacks in WSNs, which is crucially essential for security measurement. All the detection methods only detect one or two attacks. None of them detects an attack with the consideration that other attacks could exist and may happen at the same time. For example, in [53], if a wormhole attack is present in the WSN and there is a strong link between two replication nodes, they can exchange the random nonce value received from other nodes and thus the method cannot take effect anymore.

Third, accuracy, effectiveness and efficiency are still a topic of interests because of limited node energy and constrained resources in WSNs. This requests lightweight detection methods with high detection accuracy. Though FPR is low, it is still nonzero. We should further decrease the FPR down to zero to prevent legitimate nodes from being revoked wrongly.

Fourth, scalability support is missed in most of existing methods. Any attack may occur in a large-scale network. An application of WSN is always employed into a large-scale area and consists of thousands and millions of sensor nodes.

Fifth, Data trustworthiness and data quality are still not well considered and ensured in most of existing methods. How to process big data collected from different sources with different quality for the purpose of detecting all potential attacks towards trustworthy security measurement is still an open issue. Few methods have consideration on compromised nodes and network dynamics. They ignored the issue of data trustworthiness. If malicious nodes pretend to be normal to transmit data normally but send false security data and alarm information, they could impact network attack detection accuracy, revoke legitimate nodes and even destroy the whole network. For example, in [52], if the central node is a compromised node, the whole network will break down. In [76], if a malicious node reports that the change rate of neighbor nodes is below a threshold, all neighbor nodes will be immediately prohibited. However, few existing methods took data quality into account. In reality, the environment could impact data quality. Legitimate nodes may send false data.

Sixth, few existing methods considered location privacy and data privacy during security data collection and attack detection. They may offend privacy consciously or unintentionally during security data collection. This issue should be solved but it could be a big challenge considering the specific characteristics of WSNs.

Seventh, a dynamic threshold setting for attack detection should be provided, but not well studied so far. Some schemes, such as [59], [63], [71], [76], set a static threshold to verify an attack. It is not appropriate for practical applications because the situation changes all the time in reality. And it is difficult to set a suitable threshold to distinguish malicious nodes with legitimate nodes effectively.

Eighth, people pay little attention to attack detection in the data link layer and the transport layer. It is not enough to only focus on security protocols and other defense mechanisms to resist attacks. For example, current MAC

protocols are not sufficient to protect WSNs from denial-of-sleep attack [18].

Ninth, almost all existing methods did not seriously consider the security properties. But it is fundamental and important for a detection method to guard against some basic attacks such as eavesdropping attack and compromised node attack, and protect security data against threats. On the contrary, applying complicated cryptographic techniques for resisting the above threats on security data could consume a lot of resources, which is not suitable for WSN.

Last but not the least, data aggregation with security and privacy protection has not yet been well studied. Data aggregation is a main technique to reduce communication overhead and node energy for security data transmission. However, security mechanisms may have a negative influence on the energy efficiency of data aggregation schemes. It is necessary to design a scheme that meets security requirements while reduces communication overhead.

5.2 Future Research Directions

Based on the open issues listed above, we propose a number of future research directions.

Data trustworthiness and data quality: Data trustworthiness and data quality in WSN are two important research topics for protecting security data from being disqualified by networking environments, malicious attacks and topological changes, and for removing or filtering unused data. In WSN attack detection, we should prevent a malicious node from revoking a normal node and acting as a monitoring node. Considering that a malicious node intentionally sends error data to interrupt the whole network, authentication, especially authentication on node trust, must be applied to identify a node. Besides, data trustworthiness should be evaluated to distinguish false data from normal data for reliable security measurement. Since radio signals used in node communications in WSNs are susceptible to its environment, such as Rayleigh fading and shadowing effects, data trust evaluation in WSNs should be seriously studied. Furthermore, a dynamic threshold should be applied to judge the quality of security data and data trust based on environmental changes.

Pure distributed detection: pure distributed detection should be investigated in WSN security measurement since it can prevent single point of failure and thus more secure. Blockchain provides a possible technical solution to realize pure distributed detection. Nodes can jointly detect attacks based on a common consensus mechanism. However, we must address the efficiency and scalability of blockchain before applying it into WSN security measurement. We believe this is a very promising research topic.

Synthesis detection: security measurement based on comprehensive attack detection is a significant research topic for WSN protection and security defence. An effective attack detection method considering only one attack may fall down in the presence of some other attacks. We should investigate new attack detection methods to figure out synthesis attacks happening simultaneously.

Scalability: we should take scalability into consideration, because wireless sensors are always deployed in a large-scale area. We need to analyze whether a detection method can be applied into an intensive scene. If it only works in a small-scale network, it may break down in reality.

Privacy preservation: data privacy and location privacy should be preserved when collecting security data in WSNs. In practice, a lightweight and efficient privacy-preserving scheme is highly expected in WSNs to solve this serious issue driven by the demands of concrete applications. In this case, cryptography-based schemes may not be applicable in WSNs. A lightweight and efficient solution is highly expected.

Lightweight protection on data: For comprehensively supporting integrity, confidentiality, authentication and non-repudiation, many cryptographic algorithms can be applied to satisfy the above-mentioned demands, but not all of them are appropriate for WSN due to its specific characteristics, such as limited energy, constrained power and low memory. A modest or lightweight security scheme needs to be devised with regard to protecting security data.

Low communication overhead: how to reduce communication overhead in security data collection and attack detection is a significant research topic. WSNs have limited resources and security mechanisms normally introduce extra communication overhead. It is necessary to design a lightweight encryption scheme or apply other methods to protect data security, which can reduce communication overhead, and thus save energy.

6. Conclusion

In this survey, we summarized the security attacks in WSNs and classified them into different types based on network layers. In order to evaluate the performance of existing attack detection methods, we proposed a series of evaluation criteria in terms of both security data collection and attack detection. We further reviewed existing detection methods against eleven types of mainstream attacks in WSNs, not only single attack, but also synthesized attack. We seriously analyzed the advantages and disadvantages of the existing works by employing the proposed criteria for the purpose of exploring open research issues and propose future research directions towards trustworthy and effective security measurement in WSNs.

Acknowledgment

This work is sponsored by the National Key Research and Development Program of China (grant 2016YFB0800704), the NSFC (grants 61672410 and U1536202), the Project Supported by Natural Science Basic Research Plan in Shaanxi Province of China (Program No. 2016ZDJC-06), the Key Lab of Information Network Security, Ministry of Public Security (grant C18614), Academy of Finland (grant 308087), and the China 111 project (grants B08038 and B16037).

REFERENCES

[1] A. Gaur, B. Scotney, G. Parr and S. Mcclean, "Smart City Architecture and its Applications Based on IoT," *Procedia Computer Science*, vol. 52, no. 1, pp. 1089-1094, 2015.

[2] S. D. Roy, S. A. Singh, S. Choudhury and N. C. Debnath, " Countering Sinkhole and Black Hole Attacks on Sensor Networks Using Dynamic Trust Management," *Proceedings - International Symposium on Computers and Communications*, Marrakech, Morocco, 2008, pp, 537-542.

[3] K. Cui, A. Kumar, N. Xavier, and S. K. Panda, "An intelligent home appliance control-based on WSN for smart buildings," *IEEE International Conference on Sustainable Energy Technologies*, Hanoi, Vietnam, 2016, pp. 282–287.

[4] N. Dessart, H. Fouchal, P. Hunel, and C. Rabat, "Simulation of large scale WSN for medical care," *The IEEE symposium on Computers and Communications*, Riccione, Italy, 2010, pp. 1115–1120.

[5] M. Amarlingam, P. K. Mishra, K. V. V. D. Prasad, and P. Rajalakshmi, "Compressed sensing for different sensors: A real scenario for WSN and IoT," *IEEE World Forum on Internet of Things*, Reston, VA, USA, 2016, pp. 289–294.

[6] M. Meghdadi, S. Ozdemir, and I. Güler, "A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks," *Iete Technical Review.*, vol. 28, no. 2, pp. 89–102, Sep. 2014.

[7] L. K. Bysani and A. K. Turuk, "A Survey on Selective Forwarding Attack in Wireless Sensor Networks," *International Conference on Devices and Communications*, Mesra, India, 2011, pp. 1–5.

[8] A. V. Pramod, M. A. Azeem, and M. O. Prakash, "Detecting the Sybil Attack in Wireless Sensor Network: Survey," *International Journal of Computers & Technology*, vol. 3, no. 1, Aug. 2012.

[9] K. Venkatraman, J. V. Daniel, and G. Murugaboopathi, "Various Attacks in Wireless Sensor Network: Survey," *International Journal of Soft Computing and Engineering*, vol. 3, no. 1, Mar. 2013.

[10] D. Martins and H. Guyennet, "Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey," *International Conference on Network-Based Information Systems*, Takayama, Japan, 2010, pp. 313–320.

[11] M. Xie, S. Han, B. Tian, and S. Parvin, "Anomaly detection in wireless sensor networks: A survey," *Journal of Network and Computer Applications*, vol. 34, no. 4, pp. 1302–1325, Jul. 2011.

[12] M. M. Patel and A. Aggarwal, "Security attacks in wireless sensor networks: A survey," *International Conference on Intelligent Systems and Signal Processing*, Gujarat, India, 2013, pp. 329–333.

[13] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler and K. Pister, "System Architecture Directions for Networked Sensors," *System architecture directions for networked sensors*, vol. 35, no. 11, pp. 93–104, Dec. 2000.

[14] A. S. Wander, N. Gura, H. Eberle, V. Gupta and S. C. Shantz, "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks," *IEEE International Conference on Pervasive Computing and Communications*, Kauai Island, HI, USA, 2005, pp. 324-328.

[15] J. Sen, "A survey on wireless sensor network security," *Computer Science*, vol. 1, no. 2, pp. 59-82, Nov. 2010.

[16] I. Tomić and J. A. Mccann, "A survey of potential security issues in existing wireless sensor network protocols," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1910–1923, Dec. 2017.

[17] M. Buettner, GV. Yee, E. Anderson and R. Han, "X-MAC: A Short Preamble MAC Protocol for Duty-cycled Wireless Sensor Networks", *4th International Conference on Embedded Networked Sensor Systems*, Boulder, CO, USA, 2006, pp. 307-320.

[18] M. Brownfield, Y. Gupta and N. Davis, "Wireless Sensor Network Denial of Sleep Attack", *Information Assurance Workshop*, West Point, NY, USA, 2005, pp. 356-364.

[19] W. Xu, K. Ma, W. Trappe and Y. Zhang, "Jamming sensor networks: attack and defense strategies," *IEEE Network*, vol. 20, no. 3, pp. 41–47, Jun. 2006.

[20] M. Smache, N. El Mrabet, J. J. Gilquijano, A. Tria, E. Riou and C. Gregory, "Modeling a node capture attack in a secure wireless sensor networks," *IEEE World Forum on Internet of Things*, Reston, VA, USA, 2016, pp. 188–193.

[21] M. Conti, R. Di Pietro, L. V. Mancini and A. Mei, "Distributed Detection of Clone Attacks in Wireless Sensor Networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 5, pp. 685–698, Aug. 2010.

[22] W. Ye, J. Heidemann and D. Estrin, "An Energy-efficient MAC Protocol for Wireless Sensor Networks", *Proceedings.Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies*, St. Louis, MO, USA, 2005, vol. 3, pp. 1567-1576.

[23] F. Liu, X. Cheng, and D. Chen, "Insider Attacker Detection in Wireless Sensor Networks," *IEEE International Conference on Computer Communications*, Barcelona, Spain, 2007, pp. 1937–1945.

[24] MM. Mohiuddin, I. Adithyan and P. Rajalakshmi, "EEDF-MAC: An Energy Efficient MAC Protocol for Wireless Sensor Networks", *International Conference on Advances in Computing*, Mysore, India, 2013, pp. 1323-1329.

[25] F. Hess, "Efficient Identity Based Signature Schemes Based on Pairings," *International Workshop on Selected Areas in Cryptography*, London, UK, 2003, pp. 310–324.

[26] C. T. Hsueh, C. Y. Wen and Y. C. Ouyang, "A Secure Scheme Against Power Exhausting Attacks in Hierarchical Wireless Sensor Networks," *IEEE Sensors Journal*, vol. 15, no. 6, pp. 3590–3602, Jun. 2015.

[27] T. Bhattashli, R. Chaki and S. Sanyal, "Sleep Deprivation Attack Detection in Wireless Sensor Network", *International Journal of Computer Applications*, vol. 40, no. 15, pp. 19-25, Feb. 2012.

[28] J. Newsome, E. Shi, D. Song and A. Perrig, "The Sybil attack in sensor networks: analysis & defenses," *International Symposium on Information Processing in Sensor Networks*, Berkeley, CA, USA, 2004, pp. 259–268.

[29] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *First IEEE International Workshop on Sensor Network Protocols and Applications*, Anchorage, AK, USA, 2003, pp. 113–127.

[30] V. Bansal and K. K. Saluja, "Anomaly based detection of Black Hole Attack on leach protocol in WSN," *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, India, 2016, pp. 1924–1928.

[31] S. P. Dongare and R. S. Mangrulkar, "Implementing energy efficient technique for defense against Gray-Hole and Black-Hole attacks in wireless sensor networks," *2015 International Conference on Advances in Computer Engineering and Applications*, Ghaziabad, India, 2015, pp. 167–173.

[32] M. Stehlík, V. Matyáš and A. Stetsko, "Towards better selective forwarding and delay attacks detection in wireless sensor networks," *2016 IEEE International Conference on Networking, Sensing, Control*, Mexico City, Mexico, 2016, pp. 1–6.

[33] N. M. Alajmi and K. Elleithy, "A new approach for detecting and monitoring of selective forwarding attack in wireless sensor networks," *IEEE Long Island Systems, Applications and Technology Conference*, Farmingdale, NY, USA, 2016, pp. 1–6.

[34] Z. Zhao, B. Wei, X. Dong, L. Yao and F. Gao, "Detecting Wormhole Attacks in Wireless Sensor Networks with Statistical Analysis," *Wase International Conference on Information Engineering*, London, UK, 2010, pp. 251–254.

[35] P. Amish and V. B. Vaghela, "Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV Protocol," *Procedia Computer Science,* vol. 79, pp. 700–707, 2016.

[36] L. Hu, "Using Directional Antennas to Prevent Wormhole Attacks," *Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, USA, 2004, pp. 1-11.

[37] I. Krontiris, T. Giannetsos and T. Dimitriou, "Launching a Sinkhole Attack in Wireless Sensor Networks; The Intruder Side," *IEEE International Conference on Wireless and Mobile Computing*, Avignon, France, 2008, pp. 526–531.

[38] Q. Jin, H. Tang, X. Kuang and Q. Liu, "Detection and defence of Sinkhole attack in Wireless Sensor Network," *IEEE International Conference on Communication Technology*, Chengdu, China, 2012, pp. 809–813.

[39] C. Y. Chong and S. P. Kumar, "Sensor networks: evolution, opportunities, and challenges," *Proceeding of the IEEE*, vol. 91, no. 8, pp. 1247–1256, Aug. 2003.

[40] S. Sharma and S. K. Jena, "A survey on secure hierarchical routing protocols in wireless sensor networks," *International Conference on Communication, Computing & Security*, Rourkela, Odisha, India, 2011, pp. 146–151.

[41] N. Gura, A. Patel, A. Wander, H. Eberle and S. C. Shantz, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs," *Cryptographic Hardware and Embedded Systems*, vol. 3156, pp. 119–132, 2004.

[42] D. J. Malan, M. Welsh and M. D. Smith, "A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography," *IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks*, Santa Clara, CA, USA, 2004, pp. 71-80.

[43] M. Thaile and O. B. V Ramanaiah, "Node Compromise Detection based on NodeTrust in Wireless Sensor Networks," *International Conference on Computer Communication and Informatics*, Coimbatore, India, 2016, pp. 1–5.

[44] R. Geetha, S. R. Anand and E. Kannan, "Fuzzy logic based compromised node detection and revocation in clustered wireless sensor networks," *International Conference on Information Communication and Embedded Systems*, Chennai, India, 2015, pp. 1–6.

[45] J. W. Ho, M. Wright and S. K. Das, "ZoneTrust: Fast Zone-Based Node Compromise Detection and Revocation in Wireless Sensor Networks Using Sequential Hypothesis Testing," *IEEE International Symposium on Reliable Distributed Systems*, Niagara Falls, NY, USA, 2011, pp. 494–510.

[46] F. Liu, X. Cheng and D. Chen, "Insider Attacker Detection in Wireless Sensor Networks," *2007. IEEE International Conference on Computer Communications*, Barcelona, Spain, 2007, pp. 1937–1945.

[47] M. Conti, R. Di Pietro, L. V. Mancini and A. Mei, "A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks," *ACM International Symposium on Mobile Ad Hoc Networking and Computing*, Montreal, Quebec, Canada, 2007, pp. 80–89.

[48] J. Newsome and D. Song, "GEM: Graph EMbedding for routing and data-centric storage in sensor networks without geographic information," *International Conference on Embedded Networked Sensor Systems*, Los Angeles, CA, USA, 2003, pp. 76–88.

[49] C. Cocks, "An Identity Based Encryption Scheme Based on Quadratic Residues," *Cryptography and Coding*, 2001, vol. 2260, no. 5, pp. 360–363.

[50] K. Xing, F. Liu, X. Cheng and D. H. C. Du, "Real-Time Detection of Clone Attacks in Wireless Sensor Networks," *The International Conference on Distributed Computing Systems*, Beijing, China, 2008, pp. 3–10.

[51] A. J. Macula, "A simple construction of d-disjunct matrices with certain constant weights," *Discrete Math*ematics, vol. 162, no. 1–3, pp. 311–312, Dec. 1996.

[52] W. Naruephiphat, Y. Ji and C. Charnsripinyo, "An Area-Based Approach for Node Replica Detection in Wireless Sensor Networks," *IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, Liverpool, UK, 2012, pp. 745–750.

[53] T. Dimitriou, E. A. Alrashed, M. H. Karaata and A. Hamdan, "Imposter detection for replication attacks in mobile sensor networks," *2015 7th International Conference on New Technologies, Mobility and Security (NTMS)*, 2016, vol. 108, pp. 210–222.

[54] L. C. Ko, H. Y. Chen and G. R. Lin, "A Neighbor-Based Detection Scheme for wireless sensor networks against node replication attacks," *International Conference on Ultra Modern Telecommunications & Workshops*, St. Petersburg, Russia, 2009, pp. 1–6.

[55] W. T. Zhu, "Node Replication Attacks in Wireless Sensor Networks: Bypassing the Neighbor-Based Detection Scheme," *International Conference on Network Computing and Information Security*, Guilin, China, 2011, pp. 156–160.

[56] W. Xu, W. Trappe, Y. Zhang and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," *International Symposium on Mobile Ad Hoc Networking and Computing*, Urbana-Champaign, IL, USA, 2005, pp. 46–57.

[57] S. Zhong, Y. G. Liu and Y. R. Yang, "Privacy-Preserving Location-based Services for Mobile Users in Wireless Networks," *Yale Computing Science*, 2004, pp. 1-13.

[58] J. Thangapoo Nancy, K. P. Vijayakumar and P. Ganesh Kumar, "Detection of jammer in Wireless Sensor Network," *International Conference on Communications and Signal Processing*, Melmaruvathur, India, 2014, pp. 1435–1439.

[59] V. C. Manju and K. M. Sasi, "Detection of jamming style DoS attack in Wireless Sensor Network," *2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing*, Solan, India, 2012, pp, 563-576.

[60] D. Murat and S. Youngwhan, "An RSSI-based scheme for sybil attack detection in wireless sensor networks," *2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks*, Buffalo-Niagara Falls, NY, USA, 2006, pp. 566-570.

[61] J. Wang, G. Yang, Y. Sun and S. Chen, "Sybil Attack Detection Based on RSSI for Wireless Sensor Network," *International Conference on Wireless Communications, Networking and Mobile Computing*, Shanghai, China, 2007, pp. 2684–2687.

[62] D. J. Huang, W. C. Teng, C. Y. Wang, H. Y. Huang and M. J. Hellerstein, "Clock Skew Based Node Identification in Wireless Sensor Networks," *Global Telecommunications Conference*, New Orleans, LO, USA, 2008, pp. 1–5.

[63] D. Prachi, S. N. Gafandeep and J. Vishal, "Detection and Prevention of Black Hole Attacks in Cluster Based Wireless Sensor Network," *International Conference on Computing for Sustainable Global Development*, New Delhi, India, 2016, pp. 3399–3403.

[64] R. Alattas, "Detecting Black-Hole Attacks in WSNs using Multiple Base Stations and Check Agents," *2016 Future Technologies Conference*, San Francisco, CA, USA, 2016, pp. 1020–1024.

[65] M. Motamedi and Y. Nasser, "Detection of Black Hole Attack in Wireless Sensor Network Using UAV," *Information and Knowledge Technology*, Urmia, Iran, 2015, pp. 1–5.

[66] A. Prathapani, L. Santhananr and D. P. Agrawal, "Intelligent honeypot agent for blackhole attack detection in wireless mesh networks," *IEEE International Conference on Mobile Adhoc and Sensor Systems*, Macau, China, 2009, pp. 753–758.

[67] J. Park, D. O. Seong, M. Yeo, B. Y. Lee and J. Yoo, "An Energy-Efficient Selective Forwarding Attack Detection Scheme Using Lazy Detection in Wireless Sensor Networks," *Lecture Notes in Electrical Engineering*, vol. 214, no. 1, pp. 157–164, Nov. 2012.

[68] RamandeepKaur and Vinodsharma, "A Survey on the Solutions for the Problems of Denial of sleep Attacks", *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 2, no. 1, pp. 2637-2643, Feb. 2014.

[69] G. Li, X. Liu and C. Wang, "A sequential mesh test based selective forwarding attack detection scheme in wireless sensor networks," *International Conference on Networking, Sensing and Control*, Chicago, IL, USA, 2010, pp. 554–558.

[70] S. Marti, T. J. Giuli, K. Lai and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," *International Conference on Mobile Computing and Networking*, Boston, MA, USA 2000, pp. 255–265.

[71] N. Dharini, R. Balakrishnan and A. P. Renold, "Distributed Detection of Flooding and Gray Hole Attacks in Wireless Sensor Network," *2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM)*, Chennai, India, 2015, pp. 178-184.

[72] J. Ren, S. Member, Y. Zhang, K. Zhang and S. Member, "Adaptive and Channel-Aware Detection of Selective Forwarding Attacks in Wireless Sensor Networks," *IEEE Transaction on Wireless Communications*, vol. 15, no. 5, pp. 3718–3731, May, 2016.

[73] T. Zaw and H. M. Aung, "Wormhole Attack Detection in Wireless Sensor Networks," *International Journal of Electrical, Computer, Energetic and Communiction Engineering*, vol. 2, no. 10, pp. 545–550, 2008.

[74] S. Subha and U. G. Sankar, "Message authentication and wormhole detection mechanism in wireless sensor network," *IEEE International Conference on Intelligent Systems and Control*, Coimbatore, India, 2015, pp. 1–4.

[75] G. Luo, Z. Han, L. Lu and M. J. Hussain, "Real-time and passive wormhole detection for wireless sensor networks," *IEEE International Conference on Parallel and Distributed Systems*, Hsinchu, Taiwan, 2015, pp. 592–599.

[76] M. M. Patel and A. Aggarwal, "Two phase wormhole detection approach for dynamic wireless sensor networks," *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, India, 2016, pp. 2109–2112.

[77] M. Garcia-Otero and A. Poblacion-Hernandez, "Detection of wormhole attacks in wireless sensor networks using range-free localization," *IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks*, Barcelona, Spain, 2012, pp. 21–25.

[78] M. Guerroumi, A. Derhab and K. Saleem, "Intrusion Detection System against Sink Hole Attack in Wireless Sensor Networks with Mobile Sink," *International Conference on Information Technology - New Generations*, Las Vegas, NV, USA, 2015, pp. 307–313.

[79] S. A. Salehi, M. A. Razzaque, P. Naraei and A. Farrokhtala, "Detection of sinkhole attack in wireless sensor networks," *IEEE International Conference on Space Science and Communication*, Melaka, Malaysia, 2013, pp. 361–365.

[80] C. Chen, M. Song and G. Hsieh, "Intrusion detection of sinkhole attacks in large-scale wireless sensor networks," *IEEE International Conference on Wireless Communications, Networking and Information Security*, Beijing, China, 2010, pp. 711–716.

[81] B. E. Brodsky and B. S. Darkhovsky, "Nonparametric methods in change-point problems," *Kluwer Academic Publishers*, vol. 243, pp. 96–104, 1993.

[82] S. Sharmila and G. Umamaheswari, "Detection of Sinkhole Attack in Wireless Sensor Networks Using Message Digest Algorithms," *International Conference on Process Automation, Control and Computing*, Coimbatore, India, 2011, pp. 1–6.

[83] C. Tumrongwittayapak and R. Varakulsiripunth, "Detecting Sinkhole attacks in wireless sensor networks," *ICROS-SICE International Joint Conference*, Fukuoka, Japan, 2009, pp. 1966–1971.

[84] D. Dallas, C. Leckie and K. Ramamohanarao, "Hop-Count Monitoring: Detecting Sinkhole Attacks in Wireless Sensor Networks," *IEEE International Conference on Networks*, Adelaide, SA, Australia, 2007, pp. 176–181.

[85] D. Wu, G. Hu and G. Ni, "Research and Improve on Secure Routing Protocols in Wireless Sensor Networks," *IEEE International Conference on Circuits and Systems for Communications*, Shanghai, China, 2008, pp. 853–856.

[86] L. B. Oliveira, H. C. Wong, M. Bern, R. Dahab and A. A. F. Loureiro, "SecLEACH - A Random Key Distribution Solution for Securing Clustered Sensor Networks," *IEEE International Symposium on Network Computing and Applications*, Cambridge, MA, USA, 2006, pp. 145–154.

[87] R. Srinath, A. V. Reddy and R. Srinivasan, "AC: Cluster Based Secure Routing Protocol for WSN," *International conference on Networking and Services*, Athens, Greece, 2007, pp. 82-86.

[88] V. Palsingh, Aishwarya S. Anand Ukey and S. Jain, "Signal Strength based Hello Flood Attack Detection and Prevention in Wireless Sensor Networks," *International Journal of Computer Applications*, vol. 62, no. 15, pp. 1–6, Jan. 2013.

[89] S. Magotra and K. Kumar, "Detection of HELLO flood attack on LEACH protocol," *IEEE International Advance Computing Conference (IACC)*, Gurgaon, India, 2014, pp. 193–198.

[90] CT. Hsueh, CY. Wen and YC. Ouyang, "A Secure Scheme Against Power Exhausting Attacks in Hierarchical Wireless Sensor Networks", *IEEE Sensor Journal*, vol. 15, no. 6, pp. 3590-3602, Feb. 2015.

[91] P. Rolla and M. Kaur, "Dynamic Forwarding Window Technique against DoS Attack in WSN," *2016 International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE)*, Ghaziabad, India, 2016, pp. 212-216.

[92] X. Y. Jing, Z. Yan and W. Pedrycz, "Security Data Collection and Data Analytics in the Internet: A Survey", *IEEE Communications Surveys and Tutorials*, to be published, DOI: 10.1109/COMST.2018.2863942.

[93] D. H. Zhou, Z. Yan, Y. L. Fu and Z. Yao, "A Survey on Network Data Collection", *Journal of Network and Computer Applications*, vol. 116, pp. 9-23, Aug. 2018.

[94] G. Q. Li, Z. Yan, Y. L. Fu and H. L. Chen, "Data Fusion for Network Intrusion Detection: A review", *Security and Communication Networks*, vol. 2018, pp, 1-16, May, 2018.

[95] H. Q. Lin, Z. Yan, Y. Chen and L. F. Zhang, "A Survey on Network Security-Related Data Collection Technologies", *IEEE Access*, vol. 6, pp. 18345-18365, Mar. 2018.

[96] G. Liu, Z. Yan and W. Pedryczc, "Data Collection for Attack Detection and Security Measurement in Mobile Ad Hoc Networks: A Survey", *Journal of Network and Computer Applications*, vol. 105, pp. 105-122, Mar. 2018.

[97] L. M. He, Z. Yan and M. Atiquzzaman, "LTE/LTE-A Network Security Data Collection and Analysis for Security Measurement: A Survey", *IEEE Access*, vol. 6, no. 1, pp. 4220-4242, Jan. 2018.

[98] C. L. Miao, W. J. Jiang, L. Su, Y. L. Li, S. X. Guo, Z. Qin, H. P. Xiao, J. Gao and K. Ren, "Cloud-Enabled Privacy-Preserving Truth Discovery in Crowd Sensing Systems", *ACM Conference on Embedded Networked Sensor Systems*, Seoul, South Korea, 2015, pp. 183-196.

[99] Y. F. Zheng, H. Y. Duan, X. L. Yuan and C. Wang, "Privacy-Aware and Efficient Mobile Crowdsensing with Truth Discovery", *IEEE Transactions on Dependable and Secure Computing (TDSC)*, to be published, DOI: 10.1109/TDSC.2017.2753245.

[100] Y. F. Zheng, H. Y. Duan, C. Wang, "Learning the Truth Privately and Confidently: Encrypted Confidence-Aware Truth Discovery in Mobile Crowdsensing", *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 10, pp. 2475-2489, Mar. 2018.

[101] Z. Yao and Z. Yan, "A trust management framework for software-defined network applications", *Concurrency and Computation: Practice and Experience*, to be published, DOI: 10.1002/cpe.4518.

Haomeng Xie received the B.Sc. degree in telecommunications engineering from Xidian University, Xi'an, China, in 2016, where he is currently continuing to pursue the Ph. D degree in cyber security. His research interests are in security, privacy preservation in social networking and security measurement in WSN.

Zheng Yan received the BEng degree in electrical engineering and the MEng degree in computer science and engineering from the Xi'an Jiaotong University, Xi'an, China in 1994 and 1997, respectively, the second MEng degree in information security from the National University of Singapore, Singapore in 2000, and the licentiate of science and the doctor of science in technology in electrical engineering from Helsinki University of Technology, Helsinki, Finland. She is currently a professor at the Xidian University, Xi'an, China and a visiting professor and Finnish academy research fellow at the Aalto University, Espoo, Finland. Her research interests are in trust, security, privacy, and security-related data analytics. Prof. Yan serves as a general or program chair for 30+ international conferences and workshops. She is a steering committee co-chair of IEEE Blockchain international conference. She is also an associate editor of many reputable journals, e.g., IEEE Internet of Things Journal, Information Sciences, Information Fusion, JNCA, IEEE Access, SCN, etc.

Zhen Yao graduated from XiDian universitey in 2013. Now, he is pursuing master degree in the State Key Laboratory on Integrated Services Networks, Xidian University. His main research direction is Software-Defined-Network application plane's trust management system.

Mohammed Atiquzzaman received the MS and PhD degrees in electrical engineering and electronics from the University of Manchester, United Kingdom. He currently holds the Edith Kinney Gaylord Presidential professorship in the School of Computer Science at the University of Oklahoma. He is the editor-in-chief of Journal of Networks and Computer Applications, founding editor-in-chief of Vehicular Communications and has served/serving on the editorial boards of various IEEE journals and co-chaired numerous IEEE international conferences including IEEE Globecom. His research interests are in communications switching, transport protocols, wireless and mobile networks, satellite networks, and optical communications. His research has been funded by National Science Foundation, NASA, US Air Force, Cisco, Honeywell and other funding agencies. Most of his Publications can be found at www.cs.ou.edu/~atiq.