Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

# Survey on Detecting the Attacks in Wireless Sensor Networks

T.Janaranjani[1], P.Balamurugan[2], V.Sharmila[3]
[1,2,3] *Computer Science and Engineering, K.S.R. College of Engineering*

**Abstract**-A wireless Sensor Network (WSN) consists of autonomous sensors which are spatially distributed in order to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. the data is then cooperatively passed through the network to a main location. Sensor node data values are transferred through multi hop data transmission models. Secure provenance verification schemes are used to authorize the data packets. Efficient Distributed Trust Model (EDTM) is integrated with provenance verification scheme for node and data level trust analysis. Packet drop attack detection process is improved with time bounded verification mechanism. When transferring the data to the base station through the intermediate node there the attack happens. To detect the attacks this paper choose provenance concept. Provenance will checks the data should be coming from the particular source or simply it gives the trust of the node.

## I. INTRODUCTION

Sensors are small devices used to capture information from environment. The main functions of sensor devices are Capture, store and transmit the sensed data. The detail about Temperature, humidity, density of carbon dioxide and pressure gets captured by sensor. The main limitation of sensor is concerned with Battery power and bandwidth. The legitimate and attackers in the network area is identified by the intrusion detection system .In Wireless Sensor Networks the Base Station (BS) is the one which makes the decision making. The packet loses attacks are usually initiated by Malicious sensor nodes. WSN security schemes are constructed with authentication, confidentiality and integrity tasks. The WSN is considered as the built of "nodes" from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Several parts possessed by each sensor network node are: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth.

### 1.1. Characteristics and Applications

Power consumption constrains for nodes using batteries or energy harvesting, Ability to cope with node failures, Mobility of nodes, Communication failures, Heterogeneity of nodes, Scalability to large scale of deployment, Ability to withstand harsh environmental conditions, Ease of use these are the characteristics of Wireless Sensor Network.

The applications of WSN are, Area monitoring, Environmental/Earth monitoring, Air quality monitoring, Interior monitoring, Exterior monitoring, Air pollution monitoring, Forest fire detection, Landslide detection, Water quality monitoring, Natural disaster prevention, Industrial monitoring, Machine health monitoring, Data logging, Industrial sense and control applications, Water/Waste water monitoring, Observation of water quality, Water distribution network management, Preventing

 

natural disaster, Agriculture, Accurate agriculture, Irrigation management, Greenhouses, Passive localization and tracking, Smart home monitoring.

## II. LITERATURE SURVEY

### 2.1. An Efficient Distributed Trust Model for Wireless Sensor Networks (2015)

Sensor node trust levels are estimated to ensure the secured data transmission over WSN. Efficient Distributed Trust Model (EDTM) is applied to estimate the trust level for each sensor node. The system integrates the communication trust, energy trust, and data trust and recommendation trust values. Trust models have been recently suggested as an effective security mechanism for Wireless Sensor Networks (WSNs). Sensor nodes trust value, which is not enough for trust evaluation due to the widespread malicious attacks. This paper proposes an Efficient Distributed Trust Model (EDTM) for WSNs. The proposed EDTM can evaluate trustworthiness of sensor nodes more precisely and prevent the security breaches more effectively EDTM is an efficient and attack-resistant trust model. The disadvantages of this paper are Packet drop attacks are not handled.

### 2.2. Effective Key Management in Dynamic Wireless Sensor Networks (2015)

The system provides data security for dynamic WSN with node mobility environment. Certificateless-effective key management (CL-EKM) protocol is used for secure communication in dynamic WSNs . Wireless sensor networks (WSNs) have been deployed for a wide variety of applications, including military sensing and tracking, patient status monitoring, traffic flow monitoring, where sensory devices often move between different locations. Securing data and communications requires suitable encryption key protocols. In this paper, it proposes a certificateless-effective key management (CL-EKM) protocol for secure communication in dynamic WSNs characterized by node mobility. The CL-EKM supports efficient key updates when a node leaves or joins a cluster and ensures forward and backward key secrecy. The CL-EKM supports efficient key updates when a node leaves or joins a cluster and ensures forward and backward key secrecy. The protocol also supports efficient key revocation for compromised nodes and minimizes the impact of a node compromise on the security of other communication links. A security analysis of this scheme shows that this protocol is effective in defending against various attacks. The disadvantages of this paper are Energy consumption is high in security process.

### 2.3.Secure and Distributed Data Discovery and Dissemination in Wireless Sensor Networks (2015)

The system supports distributed data discovery and dissemination with security. Secure and distributed data discovery and dissemination protocol allows the network owners to authorize multiple network users with different privileges. A data discovery and dissemination protocol for wireless sensor networks (WSNs) is responsible for updating configuration parameters of, and distributing management commands to, the sensor nodes. All existing data discovery and dissemination protocols suffer from two drawbacks. First, they are based on the centralized approach; only the base station can distribute data items. Such an approach is not suitable for emergent multi-owner-multi-user WSNs. Second, those protocols were not designed with security in mind and hence adversaries can easily launch attacks to harm the network. This paper proposes the first secure and distributed data discovery and dissemination protocol named DiDrip. It allows the network owners to authorize multiple network users with different privileges to simultaneously and directly disseminate data items to the sensor nodes. Moreover, as demonstrated by our theoretical analysis, it addresses a number of possible security vulnerabilities that this concept has identified.

 

Extensive security analysis show DiDrip is provably secure. The disadvantages of this paper are Data confidentiality is not supported.

### 2.4.Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks (2015)

The system performs data aggregation with security and attack handling mechanism. Iterative filtering techniques with initial approximation model are used to secure data aggregation process. Due to limited computational power and energy resources, aggregation of data from multiple sensor nodes done at the aggregating node. Such aggregation is known to be highly vulnerable to node compromising attacks. Iterative filtering algorithms hold great promise for such a purpose. Such algorithms simultaneously aggregate data from multiple sources and provide trust assessment of these sources, usually in a form of corresponding weight factors assigned to data provided by each source. In this paper, it demonstrate that several existing iterative filtering algorithms, while significantly more robust against collusion attacks than the simple averaging methods, are nevertheless susceptive to a novel sophisticated collusion attack. To address this security issue, this paper proposes an improvement for iterative filtering techniques by providing an initial approximation for such algorithms which makes them not only collusion robust, but also more accurate and faster converging. The disadvantages of this paper are Packet drop attacks are not handled.

### 2.5.Dynamic Routing for Data Integrity and Delay Differentiated Services in Wireless Sensor Networks (2015)

Multi-path dynamic routing algorithm is adapted to support data transfer with security. Integrity and delay differentiated routing (IDDR) protocol is used to provide data integrity with minimum delay factors. Malicious sensor node attacks are not handled. Applications running on the same Wireless Sensor Network (WSN) platform usually have different Quality of Service (QoS) requirements. Two basic requirements are low delay and high data integrity. However, in most situations, these two requirements cannot be satisfied simultaneously. In this paper, based on the concept of potential in physics, it proposes IDDR, a multi-path dynamic routing algorithm, to resolve this conflict. By constructing a virtual hybrid potential field, IDDR separates packets of applications with different QoS requirements according to the weight assigned to each packet, and routes them towards the sink through different paths to improve the data fidelity for integrity-sensitive applications as well as reduce the end-to-end delay for delay-sensitive ones. Using the Lyapunov drift technique, it proves that IDDR is stable. The disadvantages of this paper is Malicious sensor node attacks are not handled.

### 2.6.Revocable and Scalable Certificateless Remote Authentication Protocol with Anonymity for Wireless Body Area Networks (2015)

The system provides security and privacy for wireless body area networks (WBANs). Remote authentication protocol and certificateless cryptography methods are used for the security and privacy. To ensure the security and privacy of the patient's health status in the wireless body area networks (WBANs), it is critical to secure the extra-body communication between the smart portable device held by the WBAN client and the application providers, such as the hospital, physician or medical staff. Based on certificateless cryptography, this paper proposes a remote authentication protocol featured with nonrepudiation, client anonymity, key escrow resistance, and revocability for extra-body communication in the WBANs. First, it presents a certificateless encryption scheme and a certificateless signature scheme with efficient revocation against short-term key exposure. Then, a certificateless anonymous remote authentication with revocation is

 

constructed by incorporating the proposed encryption scheme and signature scheme. Our revocation mechanism is highly scalable, which is especially suitable for the large scale WBANs, in the sense that the key-update overhead on the side of trusted party increased logarithmically in the number of users. The main disadvantages of this paper are Packet drop attacks are not handled.

### 2.7.Privacy and Quality Preserving Multimedia Data Aggregation for Participatory Sensing Systems (2015)

Media data quality is managed under mobile wireless devices with sensing environment. Slicer framework uses k-anonymous privacy preserving scheme for participatory sensing with multimedia data. With the popularity of mobile wireless devices equipped with various kinds of sensing abilities, a new service paradigm named participatory sensing has emerged to provide users with brand new life experience. However, the wide application of participatory sensing has its own challenges, among which privacy and multimedia data quality preservations are two critical problems. Unfortunately, none of the existing work has fully solved the problem of privacy and quality preserving participatory sensing with multimedia data. In this paper, it proposes SLICER, which is the first k-anonymous privacy preserving scheme for participatory sensing with multimedia data. SLICER integrates a data coding technique and message transfer strategies, to achieve strong protection of participant's privacy, while maintaining high data quality. Two kinds of data transfer strategies, namely transfer on meet up (TMU) and minimal cost transfer (MCT). For MCT, this paper proposes two different but complimentary algorithms, including an approximation algorithm and a heuristic algorithm, subject to different strengths of the requirement. Furthermore, it has implemented SLICER and evaluated its performance using publicly released taxi traces. The disadvantages of this paper are Malicious and anonymous node attacks are not handled.

### 2.8.A Secure Data Aggregation Scheme Based on Appropriate Cryptographic Primitives in Heterogeneous Wireless Sensor Networks (2015)

Secure data aggregation scheme for sensors (sen-SDA) is adapted to provide confidentiality in data aggregation process. Additive homomorphic encryption scheme, an identity-based signature scheme and a batch verification technique are integrated in the Sen-SDA mechanism. Energy cost of transmitting a single bit of information is approximately the same as that needed for processing a thousand operations in a typical sensor node. Thus, a practical way to prolong a wireless sensor network lifetime is to reduce the sensor energy consumption in data transmissions. Data aggregation is an efficient way to minimize energy consumption on sensors. In this paper, it proposes a practical secure data aggregation scheme, Sen-SDA, based on an additive homomorphic encryption scheme, an identity-based signature scheme, and a batch verification technique with an algorithm for filtering injected false data. The disadvantages of this paper are Packet drop attacks are not handled.

### 2.9.Cost-Aware SEcure Routing (CASER) Protocol Design for Wireless Sensor Networks (2015)

The system support secure data delivery with network lifetime improvement. Cost-Aware SEcure Routing (CASER) Protocol is used to provide data security with efficient energy management model. Lifetime optimization and security are two conflicting design issues for multi-hop wireless sensor networks (WSNs) with non-replenishable energy resources. In this paper, it first propose a novel secure and efficient Cost-Aware SEcure Routing (CASER) protocol to address these two conflicting issues through two adjustable parameters: energy balance control (EBC) and probabilistic based random walking. This paper discover that the energy consumption is severely disproportional to the uniform energy deployment for the given network topology, which greatly

reduces the lifetime of the sensor networks. To solve this problem, it proposes an efficient non-uniform energy deployment strategy to optimize the lifetime and message delivery ratio under the same energy resource and security requirement. It also provides a quantitative security analysis on the proposed routing protocol. The theoretical analysis and OPNET simulation results demonstrate that the proposed CASER protocol can provide an excellent tradeoff between routing efficiency and energy balance, and can significantly extend the lifetime of the sensor networks in all scenarios. For the non-uniform energy deployment, this analysis shows that it can increase the lifetime and the total number of messages that can be delivered by more than four times under the same assumption. The disadvantages of this paper are Malicious and anonymous node attacks are not handled.

## III. PROBLEM IDENTIFICATION

From the above survey papers this paper studied the following problems: Using the Efficient Distributed Trust Model (EDTM) the trust level for each sensor node only is estimated. This paper is not suitable for Packet drop attacks handling. Inorder to provide secure communication in dynamic WSNs Certificateless-effective key management (CL-EKM) protocol is used. Energy consumption is high in security process while using this protocol.The network owners could authorize multiple network users with different privileges by means of Secure and distributed data discovery and dissemination protocol. This protocol is not supported for Data confidentiality. Iterative filtering techniques with initial approximation model are used to secure data aggregation process. But Packet drop attacks are not handled. Remote authentication protocol and certificateless cryptography methods are used for the security and privacy. This paper also not handling the packet drop attacks. SLICER integrates a data coding technique and message transfer strategies, to achieve strong protection of participant's privacy, while maintaining high data quality. This is not used to handle the Malicious and anonymous node attacks. Secure data aggregation scheme for sensors (sen-SDA) is adapted to provide confidentiality in data aggregation process. This scheme is not handle the packet drop attacks. Cost-Aware SEcure Routing (CASER) Protocol is used to provide data security with efficient energy management model. CASER Protocol is not used for handle the Malicious and anonymous node attacks are not. To overcome these problems this paper may be considered on the Secure provenance scheme with the Efficient Distributed Trust Model (EDTM).

## IV. CONCLUSION

The secure provenance verification scheme is enhanced to handle consecutive malicious node attacks. Efficient Distributed Trust Model (EDTM) is improved with security features. Integrated verification scheme is designed to authorize the node and data. Coordinated trust model is constructed with communication, energy, data and recommendation trust values. With the help of intermediate processing nodes sensor data are streamed from multiple sources. The trustworthiness of sensor data is evaluated by applying Data provenance. Secure provenance verification scheme is used to authorize sensor data packets. In packet Bloom filters (iBF) are used to encode provenance. Provenance verification and reconstruction tasks are carried out under the base station. To detect packet drop attacks extended functionality is added with Secure provenance scheme. Provenance collection algorithm and provenance verification algorithm are used in the data verification process.

## REFERENCES

[1] Jinfang Jiang, Guangjie Han, Feng Wang, Lei Shu and Mohsen Guizani, "An Efficient Distributed Trust Model for Wireless Sensor Networks", IEEE Transactions On Parallel And Distributed Systems, Vol. 26, No. 5, May 2015.
[2] Seung-Hyun SeoJongho Won, Salmin Sultana and Elisa Bertino, "Effective Key Management in Dynamic Wireless Sensor Networks", IEEE Transactions On Information Forensics And Security, Vol. 10, No. 2, February 2015.

 

[3] Daojing He, Sammy Chan, Mohsen Guizani, Haomiao Yang and Boyang Zhou, "Secure and Distributed Data Discovery and Dissemination in Wireless Sensor Networks", IEEE Transactions On Parallel And Distributed Systems, Vol. 26, No. 4, April 2015.
[4] Mohsen Rezvani, Aleksandar Ignjatovic, Elisa Bertino and Sanjay Jha, "Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks",IEEE Transactions On Dependable And Secure Computing, Vol. 12, No. 1, January/February 2015.
[5] Jiao Zhang, Fengyuan Ren, Shan Gao, Hongkun Yang and Chuang Lin, "Dynamic Routing for Data Integrity and Delay Differentiated Services in Wireless Sensor Networks", IEEE Transactions On Mobile Computing, Vol. 14, No. 2, February 2015.
[6] Hu Xiong and Zhiguang Qin, "Revocable and Scalable Certificateless Remote Authentication Protocol With Anonymity for Wireless Body Area Networks", IEEE Transactions On Information Forensics And Security, Vol. 10, No. 7, July 2015.
[7] Fudong Qiu, Fan Wu and Guihai Chen, "Privacy and Quality Preserving Multimedia Data Aggregation for Participatory Sensing Systems", IEEE Transactions On Mobile Computing, Vol. 14, No. 6, June 2015.
[8] Kyung-Ah Shim and Cheol-Min Park, "A Secure Data Aggregation Scheme Based on Appropriate Cryptographic Primitives in Heterogeneous Wireless Sensor Networks", IEEE Transactions On Parallel And Distributed Systems, Vol. 26, No. 8, August 2015.
[9] Di Tang, Tongtong Li, Jian Ren and Jie Wu, "Cost-Aware SEcure Routing (CASER) Protocol Design for Wireless Sensor Networks", IEEE Transactions On Parallel And Distributed Systems, Vol. 26, No. 4, April 2015.

 