IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

Secure Routing Protocols in WSNs: A Survey

Arpita Pateliya[1], JigneshKumar. N.Patel[2], Ketan R. Tandel[3]

PG Student, Department of ECE, SVIT, Vasad[1]

Assistant Professor Department of ECE, SVIT, Vasad[2,3]

Abstract: Wireless sensor networks are consisting large number of sensor nodes which are limited to sensing, computing, processing the data and communication capability. Due to these limitations it is important to minimize the amount of data transmission so the average lifetime of network and bandwidth utilization improved as well minimize the computational power at every node in order to improve lifetime of network. WSNs are deployed in remote and open environment to transmit the sensitive information, and sensor nodes are easily prone to malicious activity of the attackers so security is most important. Hence, wireless sensor networks protocols must be designed with security in mind. This paper gives the future research directions in secure data aggregation in wireless sensor networks.

Keywords: Wireless Sensor Networks (WSNs), Data Aggregation, Security Objectives, Attacks, Routing Protocols.

I. INTRODUCTION

Wireless sensor networks are kind of ad hoc networks. During last decade, area of WSNs has attracted the attention of researcher, scientific and industrial community. WSNs are highly distributed and consist of many number of less cost, less power, less memory and self-organizing sensor nodes [1]. The sensor nodes sense the temperature, pressure, vibration, motion, humidity, sound etc [2].

A Sensor node in WSN consists of a sensor unit, a processing unit, data storage unit, a wireless trans-receiver, an antenna and a power management unit [14]. Each node must able to gather and process the data from sensor environment and transmit these data to the sink node or base station. Wireless sensor node consisting one or mode sensor node, one base station and a number of sensor nodes. Sensors of WSNs have become increasingly very small in terms of size, more intelligent and less expensive. Sensor nodes have easily deployment characteristics in WSNs make very popular and highly suitable for emergencies, natural disaster and military operation.

Wireless Sensor Networks (WSNs) consists of any number of sensor nodes which are not bounded in any type of infrastructure. Nodes in WSN can communicate with each other by any type of data aggregation architecture. Data aggregation is used to collect data efficiently. For the data collection from the sensor environment data aggregation is used in sensor environment.

WSNs are deployed in remote and open environment to transmit the sensitive information, and sensor nodes are easily prone to malicious activity of the attackers so security is most important. Hence, wireless sensor networks protocols must be designed with security in mind. Security with data aggregation minimize the computational power of sensor networks, hence lifetime of network can be increase. WSNs have applications like forest monitoring, manufacturing, forecast systems, military surveillance, health, home, office monitoring and many intelligent and smart systems [2].

This paper organized as follows. Section II provides overview of data aggregation in wireless sensor networks the next section III provides routing in wireless sensor networks. Section IV presents analyses of different security objectives and common attacks in WSNs. Section V gives some existing secure routing protocols for WSNs. Finally, the conclusion is specified in section VI.

II. DATA AGGREGATION IN WIRELESS SENSOR NETWORK

In a typical wireless sensor network, a large number of sensor nodes collect sensed information from the environment and this information is transferred to a base station where it is processed, analyzed, and used by the particular application. In these resource constrained networks, the data between sensor node and base station processed. Such distributed in-network processing of data is generally referred as data aggregation and involves combining the data which are belonging to same phenomenon. The main objective of data aggregation is to increase the network lifetime by reducing the resource consumption of sensor nodes such as battery energy and bandwidth. While increasing network lifetime, data aggregation protocols may degrade important quality of service metrics in wireless sensor networks, such as data accuracy, latency, fault-tolerance, and security. This is trade-off between sensor network lifetime, data accuracy, latency, fault-tolerance, and security, which is challenging task for network designer. In order to solve this trade off, data aggregation techniques must tightly couple with how packets are routed throughout the network. There is tree based data aggregation and cluster based data aggregation. Different types of routing protocols existing based on the data aggregation structure [9].

III. ROUTING IN WIRELESS SENSOR NETWORKS

Routing is the process of deciding, in which direction the traffic will be send from source and destination. Furthermore, it is necessary in order to perform the data communication tasks. Routing is necessary for the data

transmission between sensor nodes and base station. Sensor node cannot directly send data packets to the destination node or base station, by the support of intermediate nodes forward data packets from one node to another before they can safely reach the destination node. In WSNs, the network layer is mostly utilized to implement the routing of the incoming data. Routing is the critical services provided to the networks. Reliability, integrating with wake/sleep schedules, Unicast, multicast and any cast semantics, Real-time, Mobility, Voids, Security, and Congestion are different key issues in wireless sensor networks [5]. As security is one of the key issues, it needs to be implementing with data aggregation in wireless sensor networks.

As WSNs are deployed in harsh environment, security must provide against the attacks. Thus, researchers, have to consider several attributes of security objectives before deploying a secure routing protocol.

For the particular application such as military surveillance and healthcare monitoring the data must be kept private and confidential. Thus, the need for achieving the security objectives is essential in order to protect important data from any disruption and malicious intent which can harm a particular subject (e.g., system, network, patient) [2].

IV. ANALYSES OF SECURITY OBJECTIVES AND ATTACKS

In WSN applications such as military and environment monitoring, security becomes a fundamental concern in designing a secure routing protocol and also a highly demanded property as all data must protected from unauthorized access. Compromising the data during routing can affect the whole network services so security requirement must be considered during the routing for many particular applications.

Sensor nodes are considered as non-tamper resistant and base station as tamper resistant. Attackers with physical access to the node can extract the data from sensor node or attacker with malicious node can eject false data to the network, so it is necessary to provide security to the network by providing proper security algorithm based on the application.

A. Security Objectives

The objective of security services in WSNs is to protect the routing information and node resources from attacks. Various security objectives [1], [2], [4], [5] in wireless sensor network such Authentication, Confidentiality, Integrity, Availability, Freshness should be considered during the routing. All security objectives discussed below.

1. Authentication:

Authentication requires that the nodes participating in the network environment are the ones which are claiming to be. Authentication allows the verification of original source of the packets, ensure the identity of the sender, and verify the network participants. This is because an adversary node can easily modify or alter data packets by injecting false packets into the transmitted messages in the particular network scenario.

2. Confidentiality:

It is crucial to ensure that the data packets are only accessible to authorized entities only. Moreover, it is essential to maintain the secrecy of important data transmitted between sensor nodes during the routing. Any information access activity is only valid to authorized parties.

3. Integrity:

Attackers have nice capabilities to alter or modify important data in the forwarded packets, integrity crucial to ensure that a data message sent from one node to another are delivered without any alteration or modification by malicious intent. Sensitive applications such as healthcare monitoring and military rely on the integrity of the data in order to function properly. This can be ensured by the use of security mechanisms such as cryptographic hash functions [1], which require obtaining a fingerprint for each digital message.

4. Availability:

Generally, WSNs are deployed in open environment so there is high magnitude of failures in the routing procedure. A single point of failure will greatly affect the availability of the network. So, to provide availability, the connectivity service offered by the WSNs should be well functioning throughout its lifetime. A number of attacks can compromise the availability of the sensor network. Moreover, such a requirement is important to ensure that the network is capable of providing services even in the presence of node or link failures and attackers.

5. Freshness:

It implies that the data are always recent and ensures that no adversary can replay old messages. This objective must considered especially when the WSNs adapt shared keys for message communication, where an adversary can launch a replay attack using old keys as the new key is being updated and then spread to all the nodes in the WSN environment.

Security objectives discussed above can become a basic guideline for researchers to define their security purposes as well as defining the kinds of attacks that they are targeting to mitigate. Thus, in order to provide routing security in wireless sensor networks, the security objectives should be taken during the designing of routing protocol for the specific application. Therefore, the implementation of security algorithm this type of security requirements is must which can defend against the attacks in WSNs. Further discussion about this the next section outlines the attacks on WSN routing.

B. Common Attacks in WSNs

Securing WSNs becomes a crucial task due to their vulnerabilities to the network attacks. However, most of the existing works in WSNs are designed without considering the security functionalities in mind [9]. The primary goal of attacker is to reduce the network efficiency by affecting the task of sensor node or routing

procedure. This can be achieved by the inserting useless traffic which called flooding or by confusing the sensor nodes to their particular tasks in the network. Attacks are classified into active and passive [2].

Passive attacks aim to obtain transmitted information by eavesdropping without disrupting the routing protocol operations. No modification has done during the transmission process. Active attacks involve the alteration process by the adversary or creation of false messages. Active attacks can be classified as external or internal [2]. In an external attack, the attacker node is not claim to be of the sensor network. In Internal attack, the attack is launched from compromised a node which is from the network itself. For a worst-case scenario; these internal attacks can be more harmful to the network than external attacks.

Attacks on wireless sensor networks are not limited to simply DoS attacks but also a variety of techniques. The other common attacks [4], [5] are (i) spoofing, altering, or replaying routing information, (ii) selective forwarding, (iii) sinkhole, (iv) Wormhole, (v) Sybil, and (vi) HELLO flood. These attacks are described briefly in the following:

1. Spoofing, altering, or replaying route information:
This attack is targeting at the routing information exchanged between nodes. This is the most direct attack against WSN routing protocol. In this kind of process, an adversary can then attract or redirect the traffic, lengthen the latency, generate routing loops or create false errors, and message forgery.

2. Sinkhole attack:
In sinkhole attack, the adversary tries to attract all the traffic from a particular area through a compromised node. A sinkhole attack mainly works by making a compromised node look attractive to the neighbouring nodes to route the data packet and generate spoof, modify or drop the packet. Moreover, the intruder targets to lure the traffic in routing towards itself, with false routing information.

3. Wormhole:
Wormhole is harmful against routing in sensor networks where the attacker receives packets at one location in the network, tunnels them over a low latency link and then replays them at different remote locations in the network. An adversary launches wormhole with two distant malicious nodes and tries to attract the traffic by showing one hop distance to the sink. This attack is very difficult to detect as it uses out-of bounds channels to route packets.

4. Sybil attack:
Sybil attack mainly works by a single node presenting multiple identities to the other nodes in the network. This kind of attack is a significant threat to many geographic and multipath routing protocols.

5. HELLO flood:
HELLO flood attack depends on the neighbor information to create routing path. An adversary rebroadcasts an overhead packet with enough power to be received by every node in the network. Moreover, many routing protocols require nodes to broadcast HELLO packets to announce themselves to their neighbor within a specific radio range. However, a receiver node may assume that the packet is uncompromised as long as it is within the same range.

These network layer security attacks can be handled through the development of appropriate secure routing protocols. The use of wireless communication makes the sensor networks more prone to security threats ranging from passive eavesdropping to active interference. Without proper security provisioning, sensor nodes are easily captured, compromised, and altered by the malicious nodes. Therefore, the next section discusses the landscape of secure multipath routing with security mechanism support proposed by sensor network routing protocols.

V. SECURE ROUTING PROTOCOL

In a typical wireless sensor network, a large number of sensor nodes collect sensed information from the environment and this information is transferred to a base station where it is processed, analysed, and used by the particular application. As sensor nodes are deployed in open environment there is security issue. Some secure routing algorithm with increasing lifetime described below:

In [3] authors introduced pairwise and triple key distribution. It share same key for two as well three nodes. If in between sender and receiver node will node forward the data then sender will consider it as a malicious. Authors proposed triple key distribution to secure forwarding and key management in clustered sensor networks which Provide integrity and secrecy. It required higher computational time as well memory.

In [6] research work extended from Iterative Filtering (IF) method in order to provide data aggregation as well security for collusion attack network. This novel approach provides trustworthiness of sensor node which makes algorithm accurate and faster. This algorithm work for cluster based networks only and there is no guarantee that this approach can protect against compromised aggregators.

Authors proposed synopsis diffusion in [7], which uses duplicate insensitive algorithms for multipath routing scheme to accurately compute aggregates (e.g., predicate count or sum). This algorithm computes true aggregation in presence of attacks. This aggregation not addresses the problem of false sub-aggregation values contributed by compromised nodes.

Synopsis is generated using bitwise OR operation for aggregation, and final message authentication code (MAC) is generated by hash function and synopsis functions. Extended Kalman filtering (EKF) mechanism is used to detect false injected data [8]. EKF with combined CUMSUM and GLR gives better sensitivity to detect the injected false data. One cannot identify the adversary when majority neighbors have been compromised.

Watermarking based approaches introduced in [10]. It gives the non- linear data as it uses mean and variance of detected amplitude. It provides end to end authenticity to the data in one way approach. Novel secure data aggregation scheme for WSNs implemented in [11] based on state-ful public key encryption and homomorphic encryption. The proposed scheme gives end-to-end confidentiality and end-to-end integrity by additive homomorphic encryption and aggregate MAC respectively.Proposed protocol [12] provides the security using digital signature, which is generated by using the hash function and RSA algorithm. This gives the authentication, correctness. This proposed energy efficient protocol increase network lifetime with decreasing in Packet Drop Ratio. Cryptography primitive is used in [13] this proposed work for security. This security algorithm finds efficiency and energy conservation of whole system and end-to-end confidentiality as well hop-by-hop authentication.

There are many techniques are existed for the secure routing protocols in wireless sensor networks to provide security objectives with increasing lifetime of networks. Soft computation techniques [15] are used in order to provide efficient data aggregation in WSNs. Security with soft computing can be used to achieve the goal. Signature based methods in [12],[14] provide integrity as well authentication in WSNs which is less expensive so it gives new research direction. Watermarking [10] based algorithms are providing authenticity. Synopsis diffusion function method [7], here one can use OR, AND, XOR, XNOR any bitwise operator of this. Homomorphic function for cryptographic key using hash function [3],[13],[11],[6] exist, which are providing security objectives, and this method are proven for integrity, confidentiality, freshness etc.

VI. CONCLUSION AND FUTURE WORK

Wireless sensor network has many advantages thus it have many applications like environmental monitoring, industrial, automation, agriculture, disaster control, automotive, structure health monitoring, security and surveillance. There are several issues in which security with life time is a big issue. This paper gives the different security objectives, common attacks and several existed secure routine schemes to provide security with better lifetime. Several existing security scheme discussed in previous section and provided new direction for research.

REFERENCES

[1]. Suat Ozdemir, Yang Xiao,"Secure data aggregation in wireless sensor networks: A comprehensive overview", computer networks, vol. 53, pp. 2022-2037,2009.

[2]. Eliana Stavrou, Andreas Pitsillides, "A survey on secure routing protocols in WSNs",computer networks, vol. 54, pp. 2215-2238, 2010.

[3]. Sushmita Ruj, Amiya Nayak, Ivan Stojmenovic,"Pairwise And Triple Key Distribution In Wireless Sensor Networks with Applications", IEEE Transactions on Computers, Vol. 62, No. 11, pp. 2224-2237, November 2013.

[4]. Jyoti Rajput, Naveen Garg," A Survey on Secure Data Aggregation in Wireless Sensor Network ", International Journal of Advanced Research in Computer Science and Software Engineering,vol. 4, Issue. 5, pp. 407-412, may 2014.

[5]. Shazana Md Zin, Nor Badrul Anuar, Miss Laiha Mat Kiah, Al-Sakib Khan Pathan," Routing protocol design for secure WSN: Review and open research issues", Journal of Network and Computer Applications,Elsevier, vol. 41, pp. 517–530, 2014.

[6]. Mohsen Rezvani, Aleksandar Ignjatovic, Elisa Bertino, 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, pp. January/February 2015.

[7]. Sankardas Roy, Mauro Conti, Sanjeev Setia, Sushil Jajodia," Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact", IEEE Transactions On Information Forensics And Security, Vol. 9, No. 4, pp. 681-694, April 2014.

[8]. Bo Sun, Xuemei Shan, Kui Wu, Yang Xiao,"Anomaly Detection Based Secure In-Network Aggregation for Wireless Sensor Networks", IEEE Systems Journal, Vol. 7, No. 1, pp. 13-25, March 2013

[9]. Mousam Dagar and Shilpa Mahajan," Data Aggregation in Wireless Sensor Network: A Survey",International Journal of Information and Computation Technology, Volume 3, Number 3, pp. 167-174, 2013.

[10]. Wei Zhang, Yonghe Liu, Sajal K. Das, Pradip De,"Secure data aggregation in wireless sensor networks: A watermark based authentication supportive approach", Pervasive and Mobile Computing,Elsevier, vol. 4, pp. 658–680, 2008

[11]. Omar Rafik Merad Boudia, Sidi Mohammed Senouci, Mohammed Feham,"A novel secure aggregation scheme for wireless sensor networks using stateful public key cryptography",Ad Hoc Netwroks, vol. 32, pp. 98-113, 2015.

[12]. Shiva Murthy G, Robert John D'Souza, and Golla Varaprasad," Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks",IEEE Sensors Journal, Vol. 12, No. 10, pp. 2941-2949,October 2012

[13]. Kyung-Ah Shim, 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, pp. 2128-2139,August, 2015.

[14]. Huang Lu, Jie Li, and Hisao Kameda "A Secure Routing Protocol for Cluster-based Wireless Sensor Networks Using ID-based Digital Signature", IEEE Communications Society, 2010.

[15]. Hevin Rajesh Dhasian, Paramasivan Balasubramanian, "Survey of data aggregation techniques using soft computing in wireless sensor networks", The Institution of Engineering and Technology, vol. 7, issue. 4, pp. 336-342,2013.

BIOGRAPHIES

Arpita C. Pateliya has received her B.Tech in Electronics and communication engineering from Dharmsinh Desai University (DDU), Nadiad, Gujarat, India, in 2010. Currently she is pursuing M.E in Communication system engineering from Gujarat Technological University, Ahmedabad, Gujarat, India. Her area of interest include wireless sensor Network, Wireless Communication and Microwave technology.

Mr. JigneshKumar N. Patel has received B.E. and M.E. degrees in Electronics & Communication Engineering from Dharmsinh Desai University (DDU), Nadiad, Gujarat, India, in 1997 and 1999, respectively. Since 1999, he is working as an Assistant Professor in SVIT, Vasad, Gujarat. His area of interests includes Digital and Analog Communication, Digital Electronics.

Mr. Ketan R. Tandel has received B.E.in Electronics & Communication Engineering from GEC-Surat, Gujarat, India in 2009 and received his M.Tech in Electronics & Communication Systems from Dharmsinh Desai University (DDU), Nadiad, Gujarat, India in 2012. Since 2012, he is working as assistant Professor in SVIT, Vasad, Gujarat. His are of intrests include computer Networks, Advance wireless Networks and Wireless Communication.