International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 1 (2018) pp. 107-112
© Research India Publications. http://www.ripublication.com

Security Attacks and Energy Efficiency in Wireless Sensor Networks: A Survey

Anil S Naik[1] **and Dr. R. Murugan**[2]
[1]*Research Scholar, Department of Computer Science & Engineering.,*
Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh– 522502, India.

Orcid Id: 0000-0003-2109-6569

[2]*Professor, Department of Computer Science & Engineering.,*
Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh– 522502, India.

Orcid Id: 0000-0003-0903-5982

Abstract

- Wireless sensor networks are emerging applications of pervasive computing, consisting of many small, low power, and intelligent sensor nodes and one or more base stations. Sensor nodes gather information in diverse settings including natural ecosystems, battlefields, and manmade environments and send the information to one or more base stations. Wireless sensor networks are power constraint networks, having limited computational and energy resources. This makes them exposed enough to be attacked by any attacker deploying more resources than any individual node or base station, which may not be a difficult job for the attacker. A typical sensor network may be comprised of potentially hundreds of nodes which may use broadcast or multicast transmission. The broadcast nature of the transmission medium is the reason why wireless sensor networks are susceptible to security attacks.

Keywords - Wireless sensor networks, Malicious, Security, Wormhole, Efficient, Energy.

INTRODUCTION

Wireless sensor networks are emerging applications of pervasive computing, consisting of many small, low power, and intelligent sensor nodes and one or more base stations. Sensor nodes gather information in diverse settings including natural ecosystems, battlefields, and man made environments and send the information to one or more base stations. Sensor nodes work under severe resource constraints such as limited battery power, computing power, memory, wireless bandwidth, and communication capability, while the base station has more computational, energy and communication resources. The figure 1.1shows the basic diagram for wireless sensor network. The base station acts as a gateway between sensor nodes and the end user [1]. Sensor network applications use a data-centric approach that views a network as a distributed system consisting of many autonomously cooperating sensor nodes, any of which may have a role in routing, data gathering, or data processing. Every node will communicate through other nodes in a sensor network to produce information-rich results (e.g., temperature and soil moisture in a certain region of the network). Furthermore, intermediate nodes can perform data aggregation and caching that is useful to reduce communication overheads. Sensor network applications can be categorized according to its operational paradigm: data gathering and event-driven. The data gathering application requires sensor nodes to periodically report their data to the base station. In the event-driven application, nodes only send data when an event of interest occurs.

Wireless sensor networks are power constraint networks, having limited computational and energy resources. This makes them exposed enough to be attacked by any attacker deploying more resources than any individual node or base station, which may not be a difficult job for the attacker. A typical sensor network may be comprised of potentially hundreds of nodes which may use broadcast or multicast transmission. The broadcast nature of the transmission medium is the reason why wireless sensor networks are susceptible to security attacks.

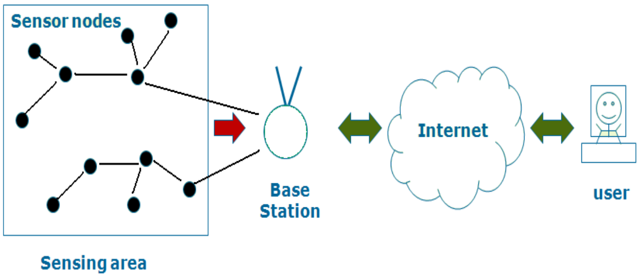

Figure 1: Wireless sensor network

A variety of attacks are possible in Wireless Sensor Network (WSN). These security attacks can be classified according to different criteria, such as the domain of the attackers, or the techniques used in attacks. These security attacks in WSN and all other networks can be roughly classified by the following criteria: passive or active, internal or external, different protocol layer, stealthy or non-stealthy, cryptography or non-cryptography related [2].

The attacker can attack the routing protocols, network traffic, inject themselves into the path between the source and destination, and thus control the network traffic flow. The traffic packets could be forwarded to a non-optimal path, which could introduce significant delay. In addition, the packets could be forwarded to a non-existent path and get lost. The attackers can create routing loops, introduce severe network congestion, and channel contention into certain areas. Multiple colluding attackers may even prevent a source node from finding any route to the destination, causing the network to partition, which triggers excessive network control traffic, and further intensifies network congestion and performance degradation [3].

The following table 1 shows the layer wise possible attacks and their impacts.

Table 1: Attacks Possible

Layers	**Attacks Possible**	**Impact**
Application Layer	SQL injection Attack	The security vulnerability within the database layer of an application layer is exploited using the SQL injection attack [4]
Transport Layer	Port Scan Attack	In order to explore the vulnerabilities of the system, the attacker finds the ports that are available using the port scan [5].
Network Layer	Denial of Service attack - SYN Flooding, Wormhole attack, Blackhole attack	A designing of a 3-way handshake which initiates a TCP connection holds the basis of SYN flooding attack. The ability of an initiator to receive packets at the IP address which was used by it as the source in initial request is verified by the third packet using this handshake [6].
Data-Link Layer	Media Access Control (MAC) Address spoofing	The known MAC address of another host is utilized for making the target switch forward frames which are destined for the remote host towards the network attacker through the MAC spoofing attacks [7].
Physical Layer	Someone can physically take away your network card or unplug your internet cable.	Don't let people touch your computer [8].

In the proposed research work a framework will be designed to protect the wireless sensor network from Selective packet dropping attack, wormhole attack, and Sybil attack, so these attacks are discussed in detail below:

Selective packet dropping attack - After compromising one or multiple sensor nodes, an intruder may launch various attacks to disrupt the in-network communication. Among these attacks, the most common one is dropping packets i.e., compromised nodes drop the packets that they supposed to forward.

Worm holes attack - In the wormhole attack, pair of awful nodes firstly discovers a wormhole at the network layer. A wormhole is a low-latency junction between two sections of a network. The malicious node receives packets in one section of the network and sends them to another section of the network. These packets are then replayed locally. This creates a fake scenario that the original sender is only one or two nodes away from the remote location. This may cause congestion and retransmission of packets squandering the energy of innocent nodes.

Sybil attack - This again is a network layer attack. In this, an awful node presents more than one character in a network. It was originally described as an attack able to defeat the redundancy mechanisms of distributed data storage systems in peer-to-peer networks. The Sybil attack is efficient enough to stroke other fault tolerant schemes such as multi path routing, routing algorithms, data aggregation, voting, fair resource allocation, and topology maintenance and misbehaviour detection. The fake node implies various identities to other nodes in the network and thus occurs to be in more than one place at a time. In this way, it disturbs the geographical routing protocols. It can collide with the routing algorithms by constructing many routes from only one node [9].

The importance of the research work is

- The research will help in the design of more secure wireless sensor network systems in the future.
- The life of sensor battery will increase as these attacks consume a large amount of sensor battery.

The proposed technique will make wireless sensor networks more reliable.

RELATED WORKS

A variety of literature is available related to intrusion detection in wireless sensor networks for selective packet dropping, wormhole, and Sybil attacks. A few of the related work is discussed below.

The paper entitled “The Sybil Attack in Sensor Networks: Analysis & defences” presents systematically analyses the threat posed by the Sybil attack to wireless sensor networks. Authors demonstrate that the attack can be exceedingly detrimental to many important functions of the sensor network such as routing, resource allocation, misbehaviour detection, etc. authors establish a classification of different types of the Sybil attack, which enables to better understand the threats posed by each type, and better design countermeasures against each type. Author then propose several novel techniques to defend against the Sybil attack, and analyses their effectiveness quantitatively [10].

The sensor networks are especially susceptible to attacks is because of their specialized communication pattern. Since all packets share a similar ultimate destination (in networks with just a single base station), a compromised node needs just to give a single brilliant route to the base station so as to influence a potentially large number of nodes. In WSN, nodes have particular properties, for example, stable neighbor's information that aides in detection of anomalies in network. Nodes monitor their neighbourhood and collaborate with cluster head to detect malicious conduct. Despite the fact that nodes don't have worldwide view however they can in any case detect an intrusion with certain probability and report to cluster head. This paper introduces a specification based Intrusion Detection System for wireless sensor networks. The proposed scheme tries to optimize the local (information collected by watch dogs) into worldwide information (decision taken by cluster head) so as to compensate the communication pattern in network [11].

The paper entitled "Survey On Selective Forwarding Attack in Wireless Sensor Networks", have discussed about selective forwarding attack, its types and some countermeasure schemes. Author concludes that Secure and on time transmission of packets is the basic need in wireless sensor network. One of the attacks that violate this need is Selective Forwarding attack. In this attack, a malicious node is dropping packets which make information unavailable. They have discussed some of the mitigation schemes to defend this attack and had given analysis on every scheme. This analysis will help us to know the drawbacks in the previous schemes and may helpful to overcome the drawbacks in the future [12].

The paper entitled "A Comparison of Link Layer Attacks on Wireless Sensor Networks", focus on security of WSNs, divide it (the WSNs security) into four categories and consider them, include: an overview of WSNs, security in WSNs, the threat model on WSNs, a wide variety of WSNs' link layer attacks and a comparison of them. The work by authors enables to identify the purpose and capabilities of the attackers; furthermore, the goal and effects of the link layer attacks on WSNs are introduced. Also, the paper discusses known approaches of security detection and defensive mechanisms against the link layer attacks; this would enable IT security managers to manage the link layer attacks of WSNs more effectively [13].

The paper entitled "Prevention of wormhole attack in wireless sensor network" investigate the techniques dealing with wormhole attacks and an approach for wormhole prevention is proposed. The approach proposed in the paper makes RREP packet forwarding conditional. By checking the validity of the two-hop neighbour node that has forwarded the packet, a node lets it to move further towards the source. Wormhole end is detected when the identity of the two-hop neighbour is found illegal. Authenticity checking of such two-hop neighbours is carried out using a preloaded secret key. By comparing the memory requirement for various numbers of neighbours, it can be concluded that by spending more on setup cost, higher scalability can be achieved. The proposed scheme focuses on the type of wormhole with out-of-band channel. It can be extended to detect other types of wormhole attacks also. [14].

The proposed in this paper that proposed in this paper wormhole is a sort of attack in Wireless Sensor Network (WSN) that needs not to crack encryption key, which has awesome harm. Aiming at characteristics of Wormhole attack, the paper presented a sort of wormhole attack defence strategy of WSN in light of neighbour nodes verification. Under this strategy, when every normal node received control packet, it will monitor the packet to figure out if it originates from its normal neighbour nodes to avoid Wormhole attack effectively. Modelling and simulation of WSN in view of OMNeT++ shows that the AODV added neighbour nodes verification effectively implement effective defence. Wormhole needs not to crack encryption key, which has extraordinary harm. Mature security protocol in traditional wired and wireless ad hoc networks can't be copied to WSN, so it needs to research on various sorts of unique potential security attack form in WSN and their defence strategies. Aiming at characteristics of Wormhole attack, the paper presented a sort of wormhole attack defence strategy of WSN in view of neighbour nodes verification. Under this strategy, when every normal node received control packet, it will monitor the packet to figure out if it originates from its normal neighbour nodes to avoid Wormhole attack effectively. Modelling and simulation of WSN in view of OMNeT++ shows that the AODV added neighbour nodes verification effectively implement effective defence [15].

The paper entitled "Detection of Packet Droppers in Wireless Sensor Networks Using Node Categorization Algorithm" proposes a simple yet effective scheme to catch packet droppers. In this scheme, a Tree on DAG (ToD) structure rooted at the sink is first established. When sensor data is transmitted along the tree structure towards the sink node, each packet sender or forwarder adds a small number of extra bits, which is called packet marks to the packet. Based on the packet marks, the sink node can figure out the dropping ratio associated with every sensor node, and then runs authors proposed node categorization algorithm to identify nodes that are packet droppers for sure, suspicious packet droppers, or no packet droppers. Proposed scheme has the following features: (i) being effective in detecting the dropping packets, (ii) low communication and energy overheads, (iii) being compatible with existing false packet filtering schemes. Extensive simulation on ns2 simulator is conducted to verify the effectiveness [16].

Wireless Sensor Network (WSN) is vulnerable to various types of security attacks where the attackers could undoubtedly intrude into the network and could bring about inexplicable destruction by disrupting the expected functionalities of the network. Severe seepage of battery may happen because of the attacks and as a result, the lifetime of the network may decrease drastically. In this paper, an energy-effective integrated Intrusion Detection System (IDS) is proposed to identify network layer Sybil attack. Our scheme spots out accurately and purges out the Sybil node which may falsely act as a genuine node. The experimental results demonstrate that the critical factor in WSN, energy is conserved more proficiently by the proposed scheme than the existing alternative methods. Likewise, accurate detection of the malicious node is conceivable spending relatively less energy. The reduction in energy consumption for the network-setup confirms to be extremely significant for WSN. The proposed approach comes extremely convenient even with densely deployed networks. In this work, detecting the presence of a solitary malicious node in the network is essentially focused. The idea could likewise assist in detecting colluding nodes in the network [17].

Wireless Sensor Network (WSN) is an emerging technology that offers awesome guarantee for various applications. The sensing capabilities combined with relatively small processing power and wireless communication makes it one of the fundamental technologies to be exploited in the future. Despite its attractive features, WSN is vulnerable to various security attacks. The constraints of WSN, for example, limited energy and memory make the security problem considerably more critical. One of the security issues of WSN is it is susceptible to Sybil attack. In this attack, the adversary forges multiple entities to disrupt the whole network. This paper addresses the problem by developing a lightweight trust system utilizing energy as a metric parameter for a hierarchical WSN. The performance evaluation of this system shows efficiency and scalability for detecting Sybil attacks in terms of true and false positive detection in a heterogeneous WSN. Besides, this system reduces the communication overhead in the network by scratching off feedback and recommendations among sensor nodes (SNs) [18].

The paper has proposed various intrusion detection systems to detect various types of active attacks on wireless sensor networks (WSNs). Selective forwarding and delay attacks are two straightforward yet compelling attacks that can disrupt the communication in WSNs. We propose two parameterized collaborative intrusion detection systems and optimize their parameters for given situations utilizing extensive simulations and multi-objective evolutionary calculations. Besides, we test the whole pursuit space to enable evaluation of evolution performance. We assess the influence of changes of the quantity of malicious nodes on the intrusion detection performance. The approach where we can choose from a set of non-dominated solutions based on current WSN application, security and different requirements anytime after the advancement process can be effortlessly adjusted to practical applications. In any case, the streamlining ought to be performed on a deliberately configured simulator with an accurate model of target WSN. Both detection methods can be effectively combined into single IDS recognizing selective forwarding and delay attacks [19].

PROBLEM FORMULATION

The wireless sensor networks are the self-configuring network in which sensor nodes sense the environmental conditions and pass the sensed information to base station. The size of the sensor nodes is very small due to which its battery is also very limited. In the recent times, various techniques have been proposed to reduce energy consumption of the network. Among the proposed techniques LEACH is the most efficient protocol for data aggregation. The modification is required to increase security of the LEACH protocol. Due to less security of the existing LEACH protocol the various types of attacks are possible which reduce the network performance in terms of various parameters. In this work, improvement in the LEACH protocol will be proposed to detect and isolate these attacks in the network.

PROPOSED SCHEME

In this work, we are working on three network layer attacks. These selective packets dropping, Sybil and wormhole attacks which greatly affects the network performance in terms of battery consumption, throughput and delay. The novel framework had been proposed through which these three attacks can be isolated from the networks. This framework will work on the wireless sensor networks. The basic assumption for the framework is that all the sensor nodes are static and location based clustering will be done in the network. The second assumption is that the cluster head will chosen using LEACH protocol and all the information sensor nodes which are within the cluster head are stored on Cluster head. The stored information is node id and distance from the cluster head in meters.

The proposed framework will first test the network for hello flood attack. The distance of each sensor node from cluster head is stored on cluster head. The new equation will be proposed through which distance between cluster head and sensor node will be calculated, if any node passing wrong distance information will be detected as malicious node. When whole network pass the hello attack test, the test is to detect malicious node which will be responsible for Sybil attack. I assume that all the nodes are registered to its cluster head and cluster heads maintain a registration table. The sink maintains the registration table to every cluster head and correspond their sensor nodes. The authentication mechanism will be proposed to verify the identity of the sensor nodes at cluster heads and cluster heads identity at sink node. The wormhole attack is the attack which increase delay in the network. To detect nodes which are responsible for triggering wormhole attack are detected with the watchdog technique. The figure 3.1 shows the flow diagram of research methodology carried out.

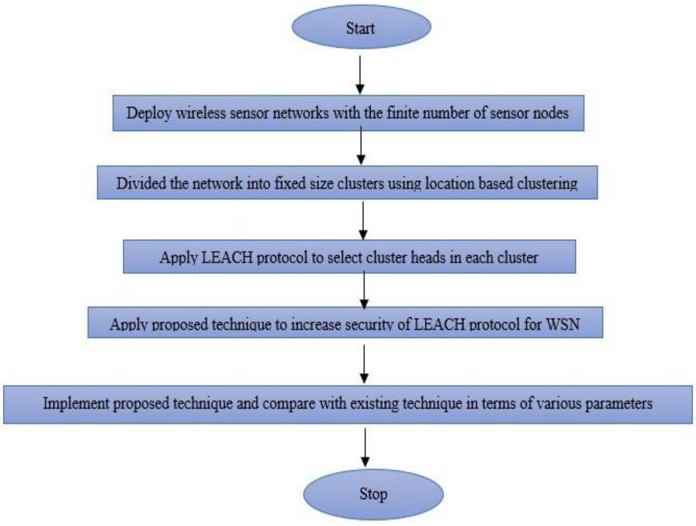
Start
Deploy wireless sensor networks with the finite number of sensor nodes
Divided the network into fixed size clusters using location based clustering
Apply LEACH protocol to select cluster heads in each cluster
Apply proposed technique to increase security of LEACH protocol for WSN
Implement proposed technique and compare with existing technique in terms of various parameters
Stop

Figure 3.1: Flow diagram

CONCLUSION

In this paper, the sensor networks are particularly susceptible to attacks is due to their specialized communication pattern. Since all packets share the same ultimate destination (in networks with only one base station), a compromised node needs only to provide a single high-quality route to the base station in order to influence a potentially large number of nodes.

we defined the Sybil attack and establish a taxonomy of this attack by distinguishing different attack types. The definition and taxonomy are very important in understanding and analysing the threat and defences of a Sybil attack. We present several novel methods by which a node can verify whether other identities are Sybil identities, including radio resource testing, key validation for random key redistribution, position verification and Registration. The most promising method among these is the random key pre- distribution which associates a node's keys with its identity. Random key pre-distribution will be used in many scenarios for secure communication, and because it relies on well understood cryptographic principles it is easier to analyse than other methods.

These methods are robust to compromised nodes. We have shown that in the multi-space pair wise scheme with each node storing 200 keys, the attacker would need to compromise 400 nodes before having even a 5% chance of being able to fabricate new identities for the Sybil attack.

LEACH is a MAC protocol, it contains many advantages like it does not need any control information, it saves energy.

REFERENCES

[1] Winnie Louis Lee, Amitava Datta, and Rachel Cardell-Oliver “Network Management in Wireless Sensor Networks,” 2010, School of Computer Science & Software Engineering, The University of Western Australia.

[2] Ray Hunt, Network Security: The Principles of Threats, Attacks and Intrusions, part1 and part 2,

APRICOT, 2004.

[3] Su-Chiu Yang, Flow-based Flooding Detection System, APRICOT,2004.

[4] Chu-Fu Wang, jau-Der Shih, Bo-Han Pan and Tin-Yu Wu, “A Network Lifetime Enhancement method for Sink Relocation and Its Analysis in Wireless sensor Networks”, 2014, IEEE Sensors Journal, Vol. 14, No. 6, 1932 - 1943.

[5] WU Xiaoping, LIN Hong and Li Gang “An Improved Routing Algorithm Based On LEACH Protocol”, 2010, Ninth International Symposium, IEEE, 259- 262.

[6] Maciej Nikodem and Bartosz Wojciechowski, “Upper Bounds on Network Lifetime for Clustered Wireless Sensor Networks”, 2011, 4th IFPI International Conference, IEEE, 1-6.

[7] Chi-Tsun Cheng, Chi K. Tse, and Francis C. M. Lau, “A Delay- Aware Data Collection Network Structure for Wireless Sensor Networks”, 2011, IEEE Sensor Journals, Vol. 11, No. 2., 699-710.

[8] Zijan Wang, and EyuphanBulut, “Energy Efficient Collision Aware Multipath Routing for Wireless Sensor Networks”, 2009, International Conference on Communications, IEEE, 1-5.

[9] Aashima Singla and Ratika Sachdeva “Review on Security Issues and Attacks in Wireless Sensor Networks,” 2013, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, ISSN: 2277 128X. Research Paper available online at: www.ijarcsse.com

[10] James Newsome, Elaine Shi, Dawn Song, and Adrian Perrig “The Sybil Attack in Sensor Networks: Analysis &Defenses,”2004, IPSN’04, April 26–27, Berkeley, California, USA.

[11] Mukesh Tiwari, Karm Veer Arya, Rahul Choudhari, Kumar Sidharth Choudhary,” Designing Intrusion Detection to Detect Black hole and Selective Forwarding Attack in WSN based on local Information”, 2009 Fourth International Conference on Computer Sciences and Convergence Information Technology

[12] Leela Krishna Bysani and Ashok Kumar Turuk “A Survey On Selective Forwarding Attack in Wireless Sensor Networks,” 2011, International conference on Devices and Communications, 24-25 February, Mesra, India. 978-1-4244-9190-2/11 ©2011 IEEE

[13] Shahriar Mohammad, Reza Ebrahimi Atani, and Hossein Jadidoleslamy “A Comparison of Link Layer Attacks on Wireless Sensor Networks,” 2011, Journal of Information Security, 2, 69-84 doi:10.4236/jis.2011 .22007 Published Online April 2011 (http://www.scirp.org/journal/jis).

[14] Dhara Buch and DeveshJinwala “Prevention of wormhole attack in wireless sensor network,” 2011, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5

[15] Jin Guo, Zhi-yong Lei,” A Kind of Wormhole Attack Defense Strategy of WSN Based on Neighbor Nodes Verification”, 2011, IEEE

[16] N. Vanitha, G.Jenifa,“ Detection of Packet Droppers in Wireless Sensor Networks Using Node Categorization Algorithm,” 2013,International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3, ISSN: 2277 128X. Research Paper available online at: www.ijarcsse.com

[17] A. BabuKaruppiah, J. Dalfiah, K. Yuvashri,” A Novel Energy-Efficient Sybil Node Detection Algorithm for Intrusion Detection System in Wireless Sensor Networks”, 2014, IEEE

[18] Noor Alsaedi, FazirulhisyamHashim, A. Sali,” Energy Trust System for Detecting Sybil Attack in Clustered Wireless Sensor Networks”, 2015, IEEE

[19] Martin Stehlik, VashekMatyas, Andriy Stetsko,” Towards Better Selective Forwarding And Delay Attacks Detection in Wireless Sensor Networks”, 2016, IEEE 13th International Conference on Networking, Sensing, and Control

[20] MostefaBendjima,” Wormhole Attack Detection in Wireless Sensor Networks”, 2016, SAI Computing Conference.

[21] Rupinder Singh, Jatinder Singh, Ravinder Singh,” TBSD: A Defend Against Sybil Attack in Wireless Sensor Networks”, 2016, IJCSNS International Journal of Computer Science and Network Security, 90 VOL.16 No.11

[22] Ju Ren, Yaoxue Zhang, Kuan Zhang, and Xuemin (Sherman) Shen,” Adaptive and Channel-Aware Detection of Selective Forwarding Attacks in Wireless Sensor Networks”, 2016, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS.

[23] Parmar Amish, V.B.Vaghela,” Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol”, 2016, Procedia Computer Science 79, 700 – 707.