IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-5, Issue-11 E-ISSN: 2347-2693

Attacks on WSN and its Limitations

Shafiqul Abidin [1*], Mohd Izhar [2]

[1*] Department of Information Technology, HMRITM (GGSIP University), Delhi, India
[2] Department of Computer Science and Engineering, HMRITM (GGSIP University), Delhi, India

*Corresponding Author: shafiqulabidin@yahoo.co.in

Available online at: www.ijcseonline.org

Received: 16/Oct/2017, Revised: 28/Oct/2017, Accepted: 14/Nov/2017, Published: 30/Nov/2017

***Abstract*—** In recent times Security has started to be the key factor in data transmission. Recent advances in networking and wireless sensing has enabled the discovery in networking and wireless sensing and has enabled the discovery of new algorithms and techniques for wireless sensor networks. A Wireless Sensor Network (WSN) comprises several sensor nodes such as magnetic, thermal, and infrared and the radar is setup in a particular geographical area. The capabilities of WSN include to manipulate and control the physical and environmental entities such as – humidity, temperature, sound, pressure, light etc. and pass this information to various other sensors present in the network in order to pass the information from the source to the sink. These wireless sensor networks have diverse applications ranging from medical care to military or educational purposes but these networks are also prone to many adversaries and attacks. Some of the most common attacks on a wireless sensor network are spoofing or replayed routing information. Certain techniques and algorithms have been introduced or developed which might not make a WSN attack-proof in all situations but may be very affective in certain situations. Selective forwarding attack is one of the most harmful attack as it can harm the complete network. A selective forwarding attack is a type of attack in which the nodes capture some data by interfering in the transmission path and steal some precious information which could be anything from secret passwords to encrypting keys and pass the rest to the destined node. The ability of capturing the required data and passing the rest of the information to the sink makes it undetectable in a network. In WSN certain techniques and algorithms have been introduced to detect selective forwarding attacks.

***Keywords*—** Authentication; Privacy; Sybil; Cryptographic Methodologies; Wireless Sensor Network; WSN; Sensor; Limitations; Sink Hole; Black Hole; Selective Forwarding Attack.

I. INTRODUCTION

Network security is one of the widely used terminologies that consists of certain features such as authentication, privacy, anti-playback, non- repudiation, integrity etc. Due to dependency on the data transmission using wireless methods, risk of wireless transmission using more and more secure methods has also increased. This in turn has also paved a way to improve the data transmission in wireless sensor network.

Sensor networks collect information or data which is important to include in smart network. These environments include transportation system, home, and healthcare, military, medical and many other fields' .In computer science the study of Wireless Sensor network plays a very important role. Wireless Sensor Networks make a huge impact on the economics which also affects the industries. A wireless sensor network may contain sensors from few tens or hundreds to more than thousands and the fact that these sensors can communicate with each other and transmit data over large distances, they play a very crucial role in some highly classified fields such as military. A sensor is basically made of four basic things or units. First is processing unit with consist of a typical microprocessor with a light operating system, sensing unit, transceiver and power unit. Nowadays many Wireless sensors have the ability to self-organize themselves for efficient transfer of data [1].

II. WSN AND ITS LIMITATIONS

In WSN sensors are arranged in order to meet the demand of a specific ad-hoc application. But the connectivity of these sensors is not static or it cannot remain unchanged in a network at any particular instant [2]. Basically, a broadcasting network is a sensor network where any signal or node can be seized by any kind and number of adversaries at any instant. This makes the wireless sensor network very vulnerable and prone to attacks as compared to other wired networks. This a big challenge for people who want to improve the network and make it more secures.

Some of the important key concepts like data confidentiality, data integrity and data privacy were also discussed in its

literature. During run time in the real environment, a complex encryption algorithm greatly effects the performance of rest of the process in the operating system. On such a restricted platform only a few space for computing and processing can be provided to other security and cryptographic algorithms. The main reason is because of some inexpensive and poor algorithms are the owner of such sensors [3].

A. Energy Limittaions

Energy is a very important constraint in a wireless sensor network. It is basically categorized in three parts. The parts are Sensor transducer, Microprocessor computations and Communication among sensor nodes. In any wireless sensor network the computation is usually less expensive as compared to the communications. It was also observed that upper security levels in wireless sensor networks usually consume more power and energy as compared to lower security levels. Hence we can say that the security levels can be distinguished on the bases of energy levels of that network [4].

B. Unreliable Communication

It can become a very harmful threat to a network sensor security. Normally protocols which are connectionless usually become unreliable. Packets may get damaged due to their transmission from a highly congested route/path or node which also leads to channel errors. A congested node may also lead to unreliable communication between the sensors of the network. Simple error handling might decrease the unreliability of a sensor network but in return generates high overheads. It is seen that though in some situations the communication channel may be reliable but the communication may not be possible. Due to the broadcasting nature, some packets might even collide with each other during transmission which results in retransmission of data [5].

C. Limittaion Associated with Memory

A sensor comprised of a tiny device powered by microprocessor and memories. Due to their small size and limited functionality they contain very low memory space within them. Usually a flash memory is used for storing the applications being downloaded. Sometimes it is not possible to run complicated operating systems. For example, tinyOS leaves even less than 4KB of memory for security and even applications use about 4KB of instructions. This is the reason why certain algorithms are not feasible for these sensors.

D. Higher Latency in Communicationy

In any wireless sensor network, techniques like multi hopping may achieve higher latency which usually occurs due to processing intermediate nodes and network congestion. This makes the network synchronization very difficult. In many security methodologies, synchronization is an important key factor and in such a case it may also lead to some serious issues in security.

III. ATTACKS ON WSN AND THEIR CLASSIFICATION

Any wireless sensor network may contain any number of sensors ranging from few hundreds to thousands and even more which may be spread over a large area. These sensors as discussed are very small and contain limited capabilities of computation and communication and are powered by batteries. This makes these sensors prone to many kinds of attacks. Practically it is not possible to monitor each and every sensor in a network which contains thousands of them. Attacks on sensors in a network are classified into transportation layer, physical layer, network layer and application layer. Typical attacks and possible defense techniques are described below [1][6].

Table 1. Attack and Approach

LAYER	ATTACKS	SECURITY APPROACH
Network Layer	Eavesdropping, Packet Rerouting, Bogus Tunnel	Authentication
Transportation Layer	Selective Forwarding Attacks and Draining Energy	Authentication on Transmission
Application Layer	Attacks on Reliability and Authenticity	Good Cryptographic Methodologies
Physical Layer	Tampering and Jamming	MAC Layer Admission Control and certain spectrum techniques can be used.

A. Energy Limittaions

The attacker can be seen in more than one position simultaneously [7]. Therefore Sybil attack is a threat to a geographical and locations based protocols and routing. This is very difficult to identify the actual attacking node. This includes large-scale, distributed, decentralised and several other types of protocols in WSN are primarily susceptible to such attacks. Earlier known as pseudo spoofing, a particular sensor node unjustifiably claims multiple identities and resides at multiple places in the networking environment. The Sybil Attack has three orthogonal extending dimensions: direct v/s indirect communication, fabricated v/s stolen identities and simultaneity. Such type of attacks necessitates a one-to-one correspondence between the sensor nodes and their individual identities. Sybil attack can be used to initiate the attack on several types of protocols in WSN such as distributed protocols, data aggregation, misbehaviour detection, voting, fair resource allocation protocols and the routing protocols [8] [9].

B. Wormhole

As the name suggests, just like a wormhole this type of attack creates a tunnel or a secret channel for transmission of data. In this type of attack an adversary simply tunnels or

channels the messages or transmitting data received from one part of the network over a low potential link and resumes them in another part. This attack can even mess up the complete message being conveyed if the adversary is situated near the base station. This can also create a sinkhole where the adversary node provides falsely a high quality route to the base station and then draw potentially all the traffic towards itself provided that other routes in the network are not that attractive.

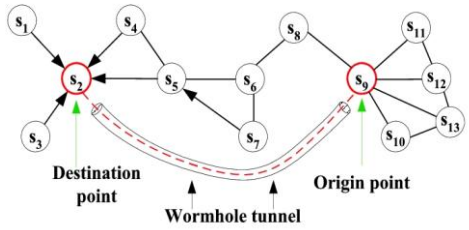

Figure 1. Wormhole Attack

C. Selective Forwarding Attacks

Usually multi hop technique is used as a mode of communication between various nodes in a wireless network using certain data gathering protocols. But this method assumes that the nodes between which the data is being transmitted is completely faithful and that they cannot be attacked or corrupted. However, in practice all the nodes are vulnerable to any kind of attacks. Selective forwarding attack which is a network layer attack is a kind of attack in which the adversary node interrupts the transmission signal by either dropping some data or completely dropping the packets thereby creating a wormhole or a black hole. These attacks are most affective when the attacking nodes are included in the path of data flow. This method may not work efficiently as now certain algorithms enable the nodes to identify the unusual behavior of their neighbor node. However, if the attacker succeeds in gathering a limited data and transfer the rest to its destined sink, he/she may become undetectable [10].

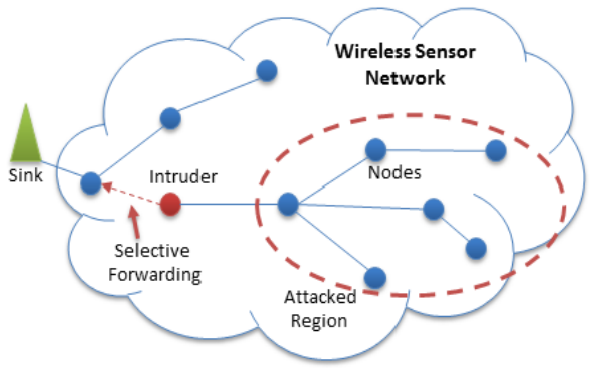

Figure 2. Black Hole Attacks

D. Analysis of Traffic

Traffic analysis attacks are created where the base station is identified by observing the data flow traffic or by observing that the majority of packets being transmitted or routed to a particular node [8]. In this attack if the attacker succeeds in identifying the base station and compromise it then it can make the network hopeless. It paves the way for the attacker to monitor the complete flow of data from any node to any other node, what data is flowing, how much data is flowing etc.[11].

E. Spoofing, Altering and Replayed Routing

This is the most common attack against a routing protocol [1]. This type of attack is used to target the transmitting info which is being switched between two nodes. The adversary may be able to create routing loops, attract or repel traffic etc. The solution to such type of attract is proper authentication [12].

IV. Selective Forwarding and its Classification

This is basically one of the prominent attacks on network layer. The packets are sent by nodes to its surrounding nodes. They consider that the forwarding messages have been sent reliably and faithfully to the destination. In selective forwarding attack, malicious nodes either drop the packages partially or completely. Though this is a simple kind of attack but can become very harmful when the malicious node acts like a wormhole or a black hole [8]. But when the attacker tries to inject such kind of attack, the neighboring nodes detect the malicious node which is completely dropping the packets and the attacker can be excluded. However the more refined form of the network is when the node is partially dropping the packets which make it difficult for other nodes to detect it [13].

The nature of dropping packets decides the classifications of selective forwarding attack. There are two types of attacks - Attack in which packets are dropped from specified nodes; Attack in which packets are dropped of some specific type.

V. Result and Conclusion

The development of certain algorithms and designs has actually increased the overall security of wireless sensor networks if not in all the fields then in specific fields. The methods allow us to make wireless sensor networks more secure and help us in improving and refining the techniques of data or information transmission. Introduction of new methodologies and advancement in existing ones have helped us in reducing the limitations such as memory consumption, poor security measures, high energy consumption to a large extent and paved a way to even detect

and defend the wireless sensor networks attacks not only simple ones but some refined ones such as SELECTIVE FORWARDING ATTACKS or black holes or wormholes which are otherwise extremely difficult to even detect. All these methods have made our wireless communication even more secure.

A selective forwarding attack is a type of attack in which the nodes capture some data by interfering in the transmission path and steal some precious information which could be anything from secret passwords to encrypting keys and pass the rest to the destined node. The ability of capturing the required data and passing the rest of the information to the sink makes it undetectable in a network.

REFERENCES

[1] Shafiqul Abidin "*WSN : Confidentiality, Integrity, Authenticity and Freshness (CIAF)*".

[2] Geethu P C,Rameez Mohammed A."*Defence Against Selective Forwarding Attack in Wireless Sensor Networks*".IEEE-2013,4th ICCCNT-2013,july 4-6,Tiruchengode, India.

[3] Naser M Alajmi, Khaled M. Elleithy."*Selective Forwarding Detection(SFD) in Wireless Sensor Networks"*.

[4] Binod Kumar Mishra,Mohan C. Nikam,Prashant Lakkadwala."*Security Against Black Hole Attack In Wireless Sensor Network-A Review*". 2014 Fourth Conference on Communication Sustems And Network Technologies"IEEE-2014.

[5] V. Subramonian, H-M. Huang, S. Datar, and C. Lu, "Priority Scheduling in tinyos case study,".*Department of Computer Science*,Washington University, St. Louis. MO.

[6] Shafiqul Abidin, "*A Novel Construction of Secure RFID Authentication Protoco*l", International Journal of Security, Computer Science Journal, Malaysia, Vol. 8, Issue 8, pp33-36, October 2014.

[7] S.Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck, M.B. Srivastava, "*On communication security in wireless adhoc sensor networks,*" in proceedings of 11th IEEE International Workshop on Enablimg Technologies: Infrasturcture for Collaborative Enterprises(WETICE'02),2002,pp.139-144.

[8] Mayank Saraogi, "*Security In Wireless Sensor Networks* ", University of Tennessee, Knoxville.

[9] Abhishek Jain, Kamal Kant and M. R. Tripathy, "*Security Solutions for Wireless Sensor Networks*" 2012, Second International Conference on Advanced Computing & Communication Technologies.

[10] I. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, *"Wireless sensor networks: A survey*". Computer Networks, 38(4):393-422.

[11] P. Sengar, N. Bhardwaj, "*A Survey on Security and Various Attacks in Wireless Sensor Network*", International Journal of Computer Sciences and Engineering, Vol.5, Issue.4, pp.78-84, 2017.

[10] J. Hill , R Szewczyk, A. Woo, S. Hollar, D.E. Culler, K. Pister, "*System architecture directions for networked sensos*". Proceedings of 9th International Conference On Architectural Support for Programing Languages and Operating Systems, New York, ACM Press 2000,pp 93-104.

[12] Manu Ahuja and Shafiqul Abidin "*Performance Analysis of Vehicular Ad-hoc Network*", International Journal of Computer Applications, USA, Vol 151 - No. 7, pp 28-30, October 2016.

[13] Bulbenkiene, V., Jakovlev, S., Mumgaudis, and G., Priotkas, G., *"Energy loss model in Wireless Sensor Networks*," IEEE Digital Information Processing and communication (ICDIPC), 2012 Second International conference, PP 36-38, 10-12 July 2012.

Authors Profile

Shafiqul Abidin is presently associated with H M R Institute of Technology & Management (Affiliated with Guru Gobind Singh Indraprastha University), Delhi, India.

Mohd Izhar is presently working in HMR Institute of Technology & Management (Affiliated with Guru Gobind Singh Indraprastha University), Delhi, India.

