International Journal on Recent Researches in Science, Engineering & Technology (IJRRSET)

A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. Journal Indexed in JIR, DIIF and SJIF.

Research Paper

Available online at: www.jrrset.com

UGC Approved Journal No: 45483

Received on: 06.02.2018 Published on: 28.02.2018 Pages : 80 - 84

ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105

Volume 6, Issue 2
February 2018.
JIR IF : 2.54
DIIF IF : 1.46
SJIF IF : 1.329

A BRIEF REVIEW ON SECURITY ATTACKS IN WIRELESS SENSOR NETWORKS

Dr.B.Rajan
IES College of Engineering, Thrissur, Kerala, India

Abstract— Wireless sensor networks are utility unique networks which range from normal ad-hoc networks for its sensing, nature of deployment of nodes and the verbal exchange paradigm. The restrained sources in wireless sensor networks are usually a key undertaking for its security. This makes them impractical to without delay follow the normal safety mechanisms as such. This paper gives a evaluation on the security threats in wireless sensor networks, specifically focusing on the routing layer the place the routing mechanisms and statistics transmission protocols are huge .This furnish research instructions in more routing solutions for protection assaults issues.

Index Terms— Wireless sensor networks, sensor nodes, security goals, protection attacks

I. INTRODUCTION

Wireless sensor community is an infrastructure less community consist of thousands and thousands of low-cost, low-power, multifunctional gadgets referred to as sensor nodes that are small in measurement and can talk over short distances [1]. These tiny sensor nodes consist of sensing, facts processing, and communicating aspects that are expert to display the real-world environment. The sensor node, sink node, the consumer node constitute the distinctive elements of a sensor network. Sensor node is the basis of the entire network. They are responsible for the appreciation of data, processing data, storage of data, transmission of statistics and forwarding of records to neighboring nodes in a cooperative manner. A sensor node monitors the network after deployment, observe any tournament of pastime queried by way of the sink and generate a report. The reviews are transmitted to the base station through multi-hop wireless channel. The BS tactics the document and sends it to the external world via high pleasant wired or wi-fi links. Thus sink serves as gateway between external world and the WSN. The sensed records includes temperature, humidity, light condition, vehicle movement, pressure, mechanical pressure strength, the speed of the airflow path and different characteristics. Sensor nodes (SNs) are typically static in nature whilst cellular nodes can be deployed based totally on the utility requirements. The sink node in the network can both be cell or static. One of the important aspects of wireless sensor networks is self-organization mechanism [4] to configure the community by way of finding out the neighboring nodes and routing table. In some purposes where wireless sensor nodes are mobile, sensor nodes can also give up working because its strength gets consumed quicker or due to other failures. Scalability of sensor nodes is some other feature. Sensor networks range from several nodes to thousands. The deployment density is additionally unique for distinct applications. For sensing and collecting data, the node density would possibly attain the degree the place a node has a number of thousand other nodes in their transmission range. The protocols related in sensor networks want to be handy to these stages and be capable to maintain desirable performance. When a node cannot immediately talk with the gateway, they use multihop routing via different nodes for the transmission. Ad-hoc wireless networks and wi-fi sensor networks have some similarities in their infrastructure much less nature and multihop routing etc. But the quantity of sensor nodes in a wireless sensor community can be quite a few orders of magnitude than the nodes in a wireless advert hoc network. Wireless sensor nodes are densely deployed and they are in charge to failure. Moreover, the topology may trade very frequently .Sensor nodes more often than not use broadcasting patterns whereas normal networks are based on point-to-point communication [3], [5].Moreover, the factor that distinguishes wi-fi sensor networks from common mobile ad-hoc networks is that the aim is the detection/estimation of some events of interest, and now not simply communication. So, sensor nodes are insufficient with power, computational capabilities, and memory. So, they are prone to physical assaults as they are unprotected in unsupervised areas. Also the broadcast and fluctuating nature of wireless medium makes WSN more inclined to security threats. Wireless sensor networks have many applications in scenarios such as military target monitoring and surveillance [2], natural disaster relief, biomedical fitness monitoring, hazardous surroundings exploration, seismic sensing etc. With herbal disasters, sensor nodes can sense and realize the surroundings to forecast disasters earlier than they manifest like forest fire, weather forecasting, earthquakes and eruptions. In health applications, surgical implants of sensors can help to reveal a patient's health. . In army target monitoring and surveillance, a WSN can assist in intrusion detection and identification. two These functions can't promise for the protection of nodes to some extent, given that they are unattended in nature after they are deployed. Recent researches on wi-fi sensor network are to combine security in the plan of each and each and every thing of WSN. two The purpose of this paper is to taxonomies the universal security assaults in wi-fi sensor networks. Section II offers an overview of safety dreams in wireless sensor networks. The everyday classification of security assaults is described in section III. Section IV summarizes the attacks in routing layer and area V concludes the paper.

II. SECURITY GOALS IN WIRELESS SENSOR NETWORKS

In real world, if each and every person node in a community receives all the messages intended to it even in the presence of an adversary, that community is said to be assured by means of the security desires [6] such as information confidentiality, authenticity, integrity of data, availability and facts freshness.

Data confidentiality: Data confidentiality is an vital thing in community security. It is the capability to impervious the message from a passive attacker so that any message communicated by using network last confidential. It ensures that the statistics will no longer be leaked with the aid of unauthorized parties.

Authenticity: Data authentication verifies the identity of the senders and receivers .It ensures that the message has come from the legit user. The wireless nature of the media and the nature of unattended nodes are challenges which requires the want of authentication. Message authentication code (MAC) is used on the communicated statistics to accomplish information authentication.

Integrity of data: Data integrity ensures that the message has now not been tampered or modified by using an unauthorised person in the network. The unstable conditions due to wireless channel may purpose loss of data. Any malicious node in the community additionally causes records alteration.

Availability and Data freshness: It is vital to ensure that the statistics furnished with the aid of any network is fresh and on hand at all times. Data freshness ensures that a 1/3 birthday celebration can't replay historical messages in future. Availability is of necessary magnitude in operational applications.

III. SECURITY ATTACKS IN WIRELESS SENSOR NETWORKS

The broadcast nature of the transmission medium in wi-fi sensor networks make them inclined to safety attacks. two Furthermore, due to the fact the nodes are deployed at random in antagonistic environment, the threats become greater serious. Many classifications of safety threats in sensor networks have been done. The extra frequent classifications are given below. A. Passive Attacks

In passive attacks [7] an unsecure site visitors is continually monitored to acquire the sensitive data from the community so that this facts can be used for launching some other severe attacks. Passive attacks ordinarily act against the data confidentiality of network. two Hence, there happens disclosure of data documents and information of the customers via an unauthorised party. The network data is neither modified nor changed. Examples for passive assaults are given below:

Monitor and eavesdropping

As the title indicates the verbal exchange between nodes in a community is monitored through an adversary node to get small print related to transmitter data. Since the wireless sensor network has wi-fi transmission medium which is frequent to all the users, the monitoring and eavesdropping is a frequent kind of attack. By encrypting the data, facts shedding can be avoided. But when attacks take place together with other types of attacks, encryption cannot supply sufficient security.

Traffic analysis: Traffic evaluation is nothing however obtaining know-how about the verbal exchange patterns in a community by using the adversary user. Adversary can motive malicious harm to some element of a community or the entire community even if encryption of records has been done. Thereby sufficient records is analysed with the aid of the attacker.

Camouflage Adversaries: In a wireless sensor community some adversaries can introduce their own nodes or make some nodes compromised. These compromised nodes also recognised as camouflage nodes. They can masquerade the different sensor nodes in the network and misbehave as everyday nodes to two make fault two routing facts and can analyse the personal important points in such a way that way ahead packets from the everyday nodes through them.

Active Attacks

In energetic attack [9], an unauthorized attacker video display units the network, listen the channel two and can alter the facts stream in the conversation channel. Active attack includes denial of carrier attacks, node malfunction, node replication attacks, false node, and passive statistics gathering etc. Routing layer assaults are lively attacks which are defined in next section.

Host primarily based vs. Network based totally attacks

Host based totally assaults are in addition categorised in to three. In User compromise attack, the users are falsely assigned to disclose touchy data about the network. Example, passwords and keys of nodes. In hardware compromise, the operations tinkers the hardware in order to take out the application code, records and key stored from hardware. In the case of software operations it is a software program compromised attack. The network based totally assault deviates the protocols from its pre-planned functioning. It does now not provide services like facts availability, confidentiality, integrity and authenticity of the network.

Layer oriented assaults

Wireless sensor community has a practical layered architecture. Layered architecture two enhances the robustness of the network by way of circumscribing the interactions of layers. Each layer is vulnerable to one-of-a-kind denial-of-service attacks and the interaction between more than one layers influences the whole architecture of the community and its communication paradigm.

Physical layer

At the physical layer the assaults aim towards physical destruction of nodes and at sign frequencies which is responsible for frequency selection, carrier frequency generation, sign detection, modulation, and information encryption functions. Deployment of nodes in opposed environments the place attacker can physically get right of entry to is a threat in bodily layer.

Jamming: Sensor nodes use Radio Frequency (RF) to speak each other. In jamming attacks, the malicious nodes are introduced by way of the adversary in order to continuously ship high power indicators to make the networks busy. So the essential conversation will be interrupted. Spread spectrum communication [9] like frequency hopping can be furnished to guard from jamming attacks.

Tampering: An attacker can damage or exchange sensor and computation hardware and the application codes or do away with sensitive materials like cryptographic keys to permit unrestricted get entry to to higher ranges of communication. Thereby these tampering nodes intervene in the physical get admission to of sensor nodes.

Data Link layer

The information hyperlink layer affords the point-to-point conversation get admission to to sensor nodes in the wireless media by Media Control Access (MAC), for instance CSMA. Link layer additionally offers error detection, error correction and facts encoding .The principal attacks in Link layer are two

Collision: Basically the collision [10] occurs when two or more nodes strive to get entry to the common channel for the transmission in the identical frequency simultaneously. So, the adversary will make the possibilities for make collisions in the channel. This may additionally alter the message content; or even discard the packets at the destination.

Exhaustion: Exhaustion also called non-stop channel get entry to in which attacker interrupts the channel get right of entry to via continuously sending information transmission requests over the channel. So, different nodes get starved for the channel. By the usage of environment friendly Time Division Multiplexing (TDMA), it can be averted to some extent.

Network layer

The goal of community routing layer is to provide reliable end-to-end transmission. The routing protocols have to be energy and reminiscence environment friendly but along with that they have to be healthful to protection attacks and node failures. There have been many power-efficient routing protocols proposed for sensor networks. Wireless sensor network assaults target the network layer in order to trade the course statistics from sensor nodes to the sink node. They take gain of the routing protocol that is used by way of the community in order to attract all the transmission from different nodes through the adversaries. Since Routing layer is accountable for routing of messages from nodes to nodes and nodes to sink node, any extend or drop in the packets two may also cause loss in data information. Many denial of carrier attacks take place in community layer which are described in subsequent part in detail.

IV. NETWORK LAYER ATTACKS

In network layer [11] the malicious nodes ahead the statistics packets thru them or delay them or drop the records either definitely or based on any criteria. Many forms of DoS assaults are listed below.

Sinkhole attack: Sinkhole [12] attracts all the nodes through malicious advertising that it is the sink node so that the member nodes forward the data toward them unknowingly. Sinkhole attack can either interfere with routing packets, spoof or replay route messages, or even transmit false document attacks, making the compromise node a more fascinating course to ahead their packets.

Selective forwarding attack: In selective forwarding attack [13] only positive packets are selectively dropped through the malicious node. This consequences in an unfaithful transmission of data. The selectively drop the packets both through the node ID or primarily based on time interval or packet content, size, the source node etc. or delay the transmission. The applicable information is misplaced in the communication network. In the instances the place all the packets are dropped and nothing is forwarded then it is referred to as black gap attack. Multipath routing combined with Random resolution of direction to destination can be used for limit the effect of selective forwarding attack. It is both termed as overlook and greed attack.

Wormhole attack: In wormhole attack [14] the adversary can tunnel the messages obtained in one part of the community to the different quit thru a low latency route consist of malicious nodes. Thereby misdirect the forwarding of relevant information. The far away nodes are made to show up so close to the sink node thereby exhaust the electricity quickly.

Sybil attack: In Sybil attack [15] the adversary node fools the neighbor notes through having a couple of identities and get entry to statistics of different nodes. As the adversary occurs in multiple locations the Geographic routing protocols are normally confused. Use of symmetric key may also overcome this attack.

Hello flood attack: Hello flood assault [8],[10] makes use of hey packets which are generally used in marketing communications in order to make visitors overhead. When a node receives such packet it unknowingly replies to it via sending packets. Hello flood attack is an injurious lively attack. It causes bandwidth wastage.

Spoofed, altered, replayed packets: This attack aims the routing statistics used by means of nodes. As a result, it should lead to creating routing loops, or extend the give up to stop delay. The attacker can delay, spoof [16], alter or replay the packets in order to create an overhead in the network.

V. CONCLUSION

Wireless Sensor networks have emerged as an auspicious future for many applications. In the absence of an ample security, deployment of sensor networks is prone to a variety of attacks. Sensor node's boundaries and nature of wireless communication poses unique safety challenges. The purpose of this paper is to provide a comprehensive taxonomy of the protection assaults on sensor networks and their impact on the performance of the network. Moreover, future directions for an prolonged lookup in the region of sensor network security are additionally provided.

REFERENCES

[1] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: a survey. Computer networks, 38(4), 393-422.

[2] Simon, G., Maróti, M., Lédeczi, Á., Balogh, G., Kusy, B., Nádas, A., ... & Frampton, K. (2004, November). Sensor network-based countersniper system. In Proceedings of the 2nd international conference on Embedded networked sensor systems (pp. 1-12). ACM.

[3] C. Perkins, "Ad Hoc Networks", Addison-Wesley, Reading, MA, 2000

[4] Toumpis, S., & Tassiulas, L. (2006). Optimal deployment of large wireless sensor networks. IEEE Transactions on Information Theory, 52(7), 2935-2953.

[5] Karlof, C., & Wagner, D. (2003, May). Secure routing in wireless sensor networks: Attacks and countermeasures. In Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on (pp. 113-127). IEEE.

[6] Padmavathi, D. G., & Shanmugapriya, M. (2009). A survey of attacks, security mechanisms and challenges in wireless sensor networks. arXiv preprint arXiv:0909.0576.

[7] Roosta, T., Shieh, S., & Sastry, S. (2006, December). Taxonomy of security attacks in sensor networks and countermeasures. In The first IEEE international conference on system integration and reliability improvements (Vol. 25, p. 94).

[8] Chauhan, R. K. (2017). Review on Security attacks and Countermeasures in Wireless Sensor Networks. International Journal of Advanced Research in Computer Science, 8(5).

[9] Xu, W., Trappe, W., Zhang, Y., & Wood, T. (2005, May). The feasibility of launching and detecting jamming attacks in wireless networks. In Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing (pp. 46-57). ACM.

[10] Raymond, D. R., & Midkiff, S. F. (2008). Denial-of-service in wireless sensor networks: Attacks and defenses. IEEE Pervasive Computing, (1), 74-81.

[11] Ioannou, C., & Vassiliou, V. (2016, September). The Impact of Network Layer Attacks in Wireless Sensor Networks. In Secure Internet of Things (SIoT), 2016 International Workshop on (pp. 20-28). IEEE.

[12] Krontiris, I., Dimitriou, T., Giannetsos, T., & Mpasoukos, M. (2007, July). Intrusion detection of sinkhole attacks in wireless sensor networks. In International Symposium on Algorithms and Experiments for Sensor Systems, Wireless Networks and Distributed Robotics (pp. 150-161). Springer, Berlin, Heidelberg.

[13] Shila, D. M., Cheng, Y., & Anjali, T. (2010). Mitigating selective forwarding attacks with a channel-aware approach in WMNs. IEEE transactions on wireless communications, 9(5).

[14] Hu, Y. C., Perrig, A., & Johnson, D. B. (2006). Wormhole attacks in wireless networks. IEEE journal on selected areas in communications, 24(2), 370-380.

[15] Newsome, J., Shi, E., Song, D., & Perrig, A. (2004, April). The sybil attack in sensor networks: analysis & defenses. In Proceedings of the 3rd international symposium on Information processing in sensor networks (pp. 259-268). ACM.

[16] Palattella, M. R., Accettura, N., Vilajosana, X., Watteyne, T., Grieco, L. A., Boggia, G., & Dohler, M. (2013). Standardized protocol stack for the internet of (important) things. IEEE communications surveys & tutorials, 15(3), 1389-1406.

[17] Wood, A. D., & Stankovic, J. A. (2004). A taxonomy for denial-of-service attacks in wireless sensor networks. Handbook of sensor networks: compact wireless and wired sensing systems, 739-763.

[18] Han, G., Shen, W., Duong, T. Q., Guizani, M., & Hara, T. (2014). A proposed security scheme against Denial of Service attacks in cluster-based wireless sensor networks. Security and Communication Networks, 7(12), 2542-2554.