Global Journals Inc.

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 17 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Wireless Sensor Network Security Model for D2P Attacks Using Zero Knowledge Protocol

By Mukesh Kansari & Mrs.Shikha Pandey

Rungta College of Engineering and Technology, Bhilai (C.G.), India

Abstract - Wireless sensor networks (WSNs) are innovative large-scale wireless networks that consist of distributed, low-power, small-size devices using sensors to cooperatively collect information through infrastructure less ad-hoc wireless network. These small devices used in wireless sensor nodes are called sensor nodes. They are envisioned to play an important role in a wide variety of areas ranging from critical military surveillance applications to forest fire monitoring and building security monitoring in the near future. In these networks, a large number of sensor nodes are deployed to monitor a vast field, where the operational conditions are most often harsh or even hostile. Since these networks are usually deployed in remote places and left unattended, they should be equipped with security mechanisms to defend against attacks such as node capture, physical tampering, eavesdropping, denial of service, etc. Unfortunately, traditional security mechanisms with high overhead are not feasible for resource constrained sensor nodes.

Keywords : sensor nodes, threats, wsn, attacks, security.

GJCST-E Classification : C.2.1

Wireless Sensor Network Security Model for D2P Attacks Using Zero Knowledge Protocol

Mukesh Kansari [α] & Mrs.Shikha Pandey [σ]

Abstract - Wireless sensor networks (WSNs) are innovative large-scale wireless networks that consist of distributed, low-power, small-size devices using sensors to cooperatively collect information through infrastructure less ad-hoc wireless network. These small devices used in wireless sensor nodes are called sensor nodes. They are envisioned to play an important role in a wide variety of areas ranging from critical military surveillance applications to forest fire monitoring and building security monitoring in the near future. In these networks, a large number of sensor nodes are deployed to monitor a vast field, where the operational conditions are most often harsh or even hostile. Since these networks are usually deployed in remote places and left unattended, they should be equipped with security mechanisms to defend against attacks such as node capture, physical tampering, eavesdropping, denial of service, etc. Unfortunately, traditional security mechanisms with high overhead are not feasible for resource constrained sensor nodes.

Keywords : sensor nodes, threats, wsn, attacks, security.

I. Introduction

A Wireless Sensor Network is a special type of network that consist of distributed, low-power, small-size devices using sensors to cooperatively collect information through infrastructure less ad-hoc wireless network [1]. They are envisioned to play an important role in a wide variety of areas ranging from critical military surveillance applications to building security monitoring in the near future [2]. It shares some commonalities with a typical computer network, but also exhibits many characteristics which are unique to it. The security services in a Wireless Sensor Network should protect the information communicated over the network and the resources from attacks and misbehavior of nodes. The most important security requirements in Wireless Sensor Network are listed below:

Data confidentiality: The security mechanism should ensure that no message in the network is understood by anyone except intended recipient. A sensor node should not allow its readings to be accessed by its neighbors unless they are authorized to do so.

Data integrity: The mechanism should ensure that no message can be altered by an entity as it traverses from the sender to the recipient.

Data freshness: It implies that the data is recent and ensures that no adversary can replay old messages. This requirement is especially important when the WSN nodes use shared keys for message communication, where a potential adversary can launch a replay attack using the old key as the new key is being refreshed and propagated to all the nodes in the WSN.

Self-organization: Each node in a WSN should be self organizing and self-healing. The dynamic nature of a WSN makes it sometimes impossible to deploy any preinstalled shared key mechanism among the nodes and the base station [3].

Secure localization: In many situations, it becomes necessary to accurately and automatically locate each sensor node in a WSN. For example, a WSN designed to locate faults would require accurate locations of sensor nodes identifying the faults. A potential adversary can easily manipulate and provide false location information by reporting false signal strength, replaying messages etc. if the location information is not secured properly. Authentication: It ensures that the communicating node is the one that it claims to be. An adversary can not only modify data packets but also can change a packet stream by injecting fabricated packets. It is, therefore, essential for a receiver to have a mechanism to verify that the received packets have indeed come from the actual sender node.

II. Charesterstics & Applications of WSNs

There is following characteristics of WSN which are-

Power consumption constrains for nodes using batteries or energy harvesting, Communication failures, Ability to cope with node failures, Mobility of nodes, Dynamic network topology, Heterogeneity of nodes, Scalability to large scale of deployment, Ability to withstand harsh environmental conditions, Easy of use Unattended operation.

Applications of WSN are-
Area monitoring,
Environmental monitoring Greenhouse
monitoring Landslide detection,
Industrial monitoring Machine

Author α : M.Tech (SE) Dept. of Computer Science and Engg. Rungta College of Engineering and Technology, Bhilai (C.G.), India.
E-mail : kansari256@gmail.com
Author σ : Assitt. Professor Dept. of Computer Science and Engg Rungta College of Engineering and Technology, Bhilai (C.G.), India.
E-mail : shikhamtech2008@gmail.com

health monitoring,
Water/Wastewater Monitoring Landfill ground well level monitoring and pump counter agriculture, Fleet monitoring, Health Monitoring Security.

III. Security Attacks in Wsn

Wireless Sensor Networks are vulnerable to various types of attacks. These attacks are mainly of three types (denial of service attack, distributed attack and phishing attack.), Attacks on secrecy and authentication: standard cryptographic techniques can protect the secrecy and authenticity of communication channels from outsider attacks such as eavesdropping, packet replay attacks. Attacks on network availability: attacks on availability of WSN are often referred to as denial-of-service (DoS) attacks. Stealthy attack against service integrity: in a stealthy attack, the goal of the attacker is to make the network accept a false data value. In these attacks, keeping the sensor network available for its intended use is essential. The DoS attack usually refers to an adversary's attempt to disrupt, subvert, or destroy a network. However, a DoS attack can be any event that diminishes or eliminates a network's capacity to perform its expected functions.

IV. Dos Attacks

Wood and Stankovic have defined a DoS attack as an event that diminishes or attempts to reduce a network's capacity to perform its expected function. Some of the important types of DoS attacks in Wireless Sensor Networks are discussed below.

a) Physical Layer Attacks

The physical layer is responsible for frequency selection, modulation, and data encryption [4]. As with any radio-based medium, the possibility of jamming is there. In addition, nodes in Wireless Sensor Networks may be deployed in hostile or insecure environments where an attacker has the physical access. Two types of attacks in physical layer are (i) jamming and (ii) tampering.

b) Link Layer Attacks

The link layer is responsible for multiplexing of data streams, data frame detection, medium access control, and error control [4]. Attacks at this layer include purposefully created collisions, resource exhaustion, and unfairness in allocation.

c) Network Layer Attacks

The network layer of Wireless Sensor Networks is vulnerable to the different types of attacks such as: spoofed routing information, selective packet forwarding, sinkhole, Sybil, wormhole, hello flood etc.

i. *Spoofed routing information*

The most direct attack against a routing protocol is to target the routing information in the network. An attacker may spoof, alter, or replay routing information to disrupt traffic in the network [5].

ii. *Selective forwarding*

Thn a multi-hop network like a Wireless Sensor Network, for message communication all the nodes need to forward messages accurately. An attacker may compromise a node in such a way that it selectively forwards some messages and drops others [5].

iii. *Sinkhole*

In this attack, a malicious node acts as a blackhole [6] to attract all the traffic in the sensor network. Especially in a flooding based protocol, the attacker listens to requests for routes then replies to the target nodes that it contains the high quality or shortest path to the base station. Once the malicious device has been able to insert itself between the communicating nodes (for example, sink and sensor node), it is able to do anything with the packets passing between them. In fact, this attack can affect even the nodes those are considerably far from the base stations. Fig 1 shows the conceptual view of a sinkhole attack.

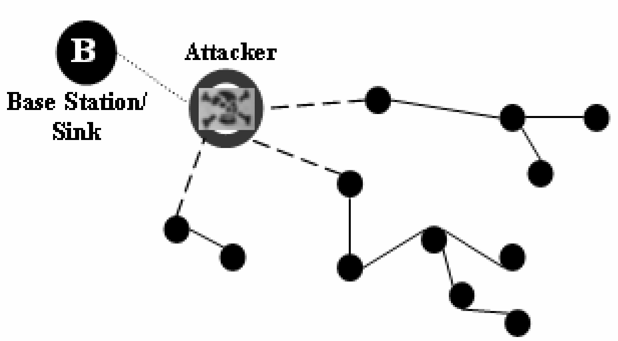

Figure 1 : Sinkhole Attack

iv. *Sybil attack*

In many cases, the sensors in a wireless sensor network might need to work together to accomplish a task, hence they can use distribution of subtasks and redundancy of information. In such situation, a node can pretend to be more than one node using the identities of other legitimate nodes. This type of attack where a node forges the identities of more than one node is the Sybil attack [7]. Sybil attack tries to degrade the integrity of data, security and resource utilization that the distributed algorithm attempts to achieve. Sybil attack can be performed for attacking the distributed storage, routing mechanism, data aggregation, voting, fair resource allocation and misbehavior detection [7]. Basically, any peer-to-peer network (especially wireless ad hoc networks) is vulnerable to Sybil attack. However, as WSNs can have some sort of base stations or gateways, this attack could be prevented using efficient protocols. Douceur [8] showed that, without a logically centralized authority, Sybil attacks are always possible except under extreme and unrealistic assumptions of resource parity and coordination among entities. However, detection of Sybil nodes in a network is not so easy.

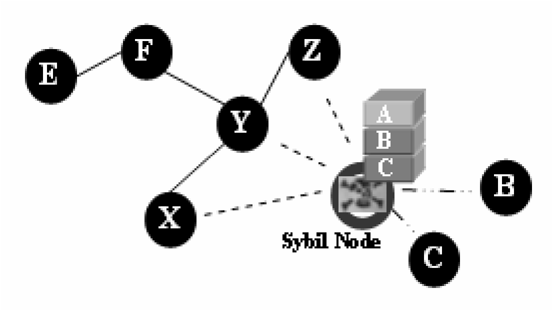

Figure 2 : Sybil Attack

v. *Wormhole*

Wormhole attack [9] is a critical attack in which the attacker records the packets at one location in the network and tunnels those to another location. The tunneling or retransmitting of bits could be done selectively. Wormhole attack is a significant threat to wireless sensor networks, because; this sort of attack does not require compromising a sensor in the network rather, it could be performed even at the initial phase when the sensors start to discover the neighboring information.

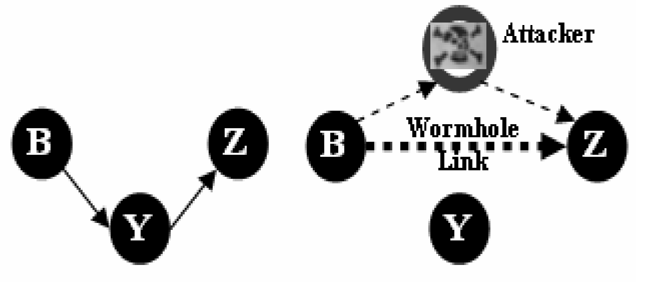

Figure 3 : Wormhole Attack

Fig 3 shows a situation where a wormhole attack takes place. When a node B broadcasts the routing request packet, the attacker receives this packet and replays it in its neighborhood. Each neighboring node receiving this replayed packet will consider itself to be in the range of Node B, and will mark this node as its parent. Hence, even if the victim nodes are multi-hop apart from B, attacker in this case convinces them that B is only a single hop away from them, thus creates a wormhole.

vi. *Hello flood*

Most of the protocols that use Hello packets make the naive assumption that receiving such a packet implies that the sender is within the radio range of the receiver. An that receiving such a packet implies that the sender is within the radio range of the receiver. An attacker may use a high-powered transmitter to fool a large number of nodes and make them believe that they are within its neighborhood [5]. Subsequently, the attacker node falsely broadcasts a shorter route to the base station, and all the nodes which received the Hello packets, attempt to transmit to the attacker node.

vii. *Acknowledgment spoofing*

Some routing algorithms for Wireless Sensor Networks require transmission of acknowledgment packets. An attacking node may overhear packet transmissions from its neighboring nodes and spoof the acknowledgments thereby providing false information to the nodes [5].

d) Transport layer attacks

The attacks that can be launched on the transport layer in a Wireless Sensor Network are flooding attack and de-synchronization attack.

i. *Flooding*

Whenever a protocol is required to maintain state at either end of a connection, it becomes vulnerable to memory exhaustion through flooding. An attacker may repeatedly make new connection request until the resources required by each connection are exhausted or reach a maximum limit. In either case, further legitimate requests will be ignored.

ii. *De-synchronization*

De-synchronization refers to the disruption of an existing connection. An attacker may, for example, repeatedly spoof messages to an end host causing the host to request the retransmission of missed frames. If timed correctly, an attacker may degrade or even prevent the ability of the end hosts to successfully exchange data causing them instead to waste energy attempting to recover from errors which never really exist.

e) Attacks on secrecy and authentication

There are different types of attacks under this category as discussed below:

i. *Node replication attack*

In a node replication attack, an attacker attempts to add a node to an existing WSN by replication the node identifier of an already existing node in the network. A node replicated and joined in the network in this manner can potentially cause severe disruption in message communication in the Wireless Sensor Network by corrupting and forwarding the packets in wrong routes.

ii. *Attacks on privacy*

Since Wireless Sensor Networks are capable of automatic data collection through efficient and strategic deployment of sensors, these networks are also vulnerable to potential abuse of these vast data sources. Privacy preservation of sensitive data in a Wireless Sensor Network is particularly difficult challenge [10]. Moreover, an adversary may gather seemingly innocuous data to derive sensitive information if he knows how to aggregate data collected from multiple sensor nodes. Following are some of the common attacks on sensor data privacy [10].

iii. *Eavesdropping and passive monitoring*

This is most common and easiest form of attack on data privacy. If the messages are not protected by cryptographic mechanisms, the adversary could easily understand the contents. Packets containing control information in a WSN convey more information than accessible through the location server, Eavesdropping on these messages prove more effective for an adversary.

iv. *Traffic analysis*

In order to make an effective attack on privacy, eavesdropping should be combined with a traffic analysis. Through an effective analysis of traffic, an adversary can identify some sensor nodes with special roles and activities in a WSN.

v. *Camouflage*

An adversary may compromise a sensor node in a WSN and later on use that node to masquerade a normal node in the network. This camouflaged node then may advertise false routing information and attract packets from other nodes for further forwarding. After the packets start arriving at the compromised node, it starts forwarding them to strategic nodes where privacy analysis on the packets may be carried out systematically.

V. Distributed Attack

A distributed attacks occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Distributed attacks are traditionally viewed to be fundamentally more difficult to detect than single-source attacks. One reason why distributed attacks are difficult to contain is because defenses against these attacks are typically deployed at edge networks, near the victim. Deploying defenses at the edge makesdetecting attacks easier,

VI. Phishing Attack

In phishing attack the hacker creates a fake web site that looks exactly like a popular site such as the SBI bank or PayPal. The phishing part of the attack is that the hacker then sends an e-mail message trying to trick the user into clicking a link that leads to the fake site. When the user attempts to log on with their account information, the hacker records the username and password and then tries that information on the real site.

VII. Challenges

There are following challenges occurring in the wireless technology which are given in the following two categories- Challenges Vs Internet:

1. Bandwidth is very expensive in WSNs
2. Ad-hoc
3. Energy
4. Wireless and Collaborative use
5. Collect and

Decimate Research Challenges:
1. Medium Access Control (MAC)
2. Routing
3. Localization
4. Operating Systems
5. Security
6. Programming Abstractions and Query Processing

VIII. Conclusion

Wireless Sensor networks have become promising future to many applications. In the absence of enough security, deployment of sensor networks is vulnerable to variety of attacks. Overall security for wireless sensor networks is very hard to develop due to the limited resources of the sensors. Sensor network security will always be a field in which much work needs to be done. Current research in sensor network security is mostly built on a trusted environment [11]; however there are several research challenges remain unanswered before we can trust on sensor networks. In this paper we have discussed threat models and unique security issues faced by wireless sensor networks. In WSNs, there are still some challenges that are to be addressed.

References Références Referencias

1. Tan f Akylidiz, Weliain S U, yogesh sankarasubramaniam and eradal caryici. ”A survey on Sensor Networks” IEEE Communication Magazine, august 2002.
2. Yuanzhu Peter Chen Arthur L. Liestman Jiangchuan Liu. ”Energy-Efficient Data Aggregation Hierarchy for Wireless Sensor Networks” Proceedings of the 2nd Int'l Conf. on Quality of Service in Heterogeneous Wired/Wireless Networks August 2005.
3. L. Eschenauer and V.D. Gligor, "A key- management scheme for distributed sensor networks", In Proceedings of the 9th ACM Conference on Computer and Networking, pp. 41- 47, Nov 2002.
4. D. Braginsky and D. Estrin, "Rumor routing algorithm for sensor networks", In Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications", pp. 22-31, New York, NY, USA, 2002, ACM Press.
5. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, May 2003, pp. 113-127.

6. Culpepper, B.J. and Tseng, H.C., “Sinkhole intrusion indicators in DSR MANETs”, Proc. First International Conference on Broad band Networks, 2004, pp. 681 – 688.
7. Newsome, J., Shi, E., Song, D, and Perrig, A, “The sybil attack in sensor networks: analysis & defenses”, Proc. of the third international Symposium on Information processing in sensor networks, ACM, 2004, pp. 259 – 268.
8. Douceur, J. “The Sybil Attack”, 1st International Workshop on Peer-to-Peer Systems (2002).
9. Hu, Y.-C., Perrig, A., and Johnson, D.B. “Packet leashes: a defense against wormhole attacks in wireless networks”, Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE INFOCOM 2003, Vol. 3, 30 March-3 April 2003, pp. 1976 – 1986.
10. M Gruteser, G. Schelle, A. Jain, R. Han, and D. Grunwald, "Privacy-aware location sensor networks", In Proceedings of the 9th USENIX Workshop on Hot Topics in Operating Systems, (HotOSIX), 2003.

This page is intentionally left blank