Types of Attacks Penetrating Wireless Sensor Networks and Strategies to Overcome Them

Payam Porkar rezaeiye[1], Maysam gharghi[2], Sassan payehdar[3], Jasem torfi[4], Hamidreza hajiaghai[5], and Pasha Porkar Rezaeiye[6]

Abstract----Like many other technologies on military and defense working on sensor networks to be started. During the Cold War, the USA's government started to sponsor the project called Sound Surveillance System. In that project the US Army trying to intrusion detection and tracking of Soviet submarines by placing a number of sensors at the strategic points under the ocean. Working on the Sensor networks project are actively started in the Defense Advanced Research Projects Agency of America since 1980 and via the distributed sensor networks project. Most of the Sensors are working with the chemical energy of a battery. Sensors can be used to intervene and penetrate to the networks. This article focuses on the methods of attack, and strategies of overcoming them.

Keywords----Wireless sensor networking, WSN, Power consumption, Energy

I. Introduction

THE sensor networks are the new generation of networks that normally are combination of a lot of enormous of cheap nodes and the relation of this node's occurred via wireless connections. The main objective in these networks is the information gathering about the network via sensors. The overall functionality of these networks is to gathering the needed information and then sending them to the receiver. Distribution of the information in this network, is instantiated, in the meaning of that the transferring of the data is done node by node. The major difference between sensor networks and ad hoc networks, is the resources of the energy and limited processing capability that is relatively low. The section 2 describes the various attacks, and the section 3 and section 4 concludes the strategies and actions to combat the attacks in the future works.

II. Current Attacks Types Can Be Categorized Into Two Types

Classifications based on device capabilities:

Class Mote: These types of attack are done by a malicious node in the network.

Class Laptop: These types of attack are done by a remote computer that is equipped with special functions.

Classifications based on the type of attackers:

External attackers: That are done by the certain equipment of the remote interferes on the network.

Internal attacker: This attack is done by a malicious node within the network.

2.1 Common types of attacks in wireless sensor networks

2-1-1 Spoof Attacking

Creating the infinitive loop of sending and receiving information, disruption of network traffic, dividing the network into several parts, and etc. are caused to disruption of the network.

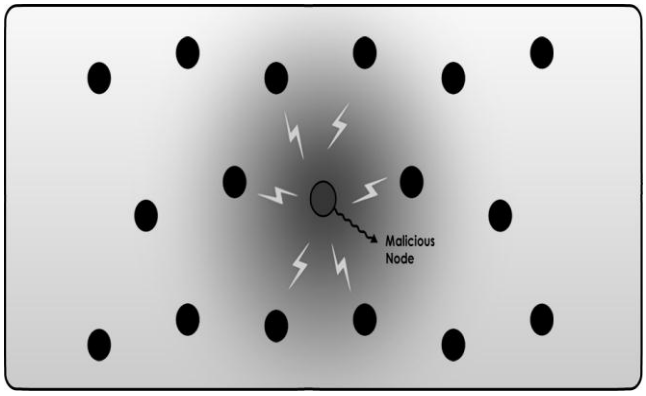

Fig. 1The Spoof Attacking

2-1-2 Selective Forwarding

In this type of attacks one or more malicious nodes placed with in the network and immediately after the receiving of information from its neighboring nodes, attempting to deflect or destroy the data, and finally, the data did not reach the main destination as well.

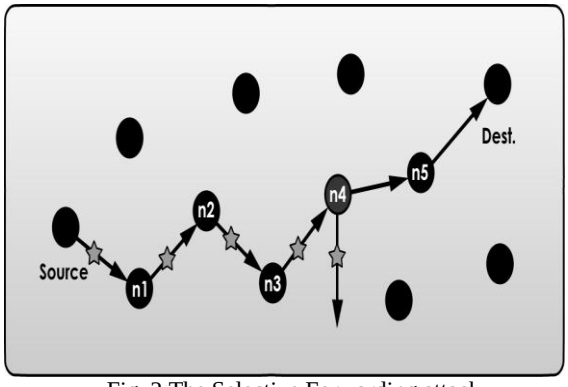

Fig. 2 The Selective Forwarding attack

[1,3,5,6]Department of computer,Damavand branch,Islamic Azad University,Damavand,Iran.

[2,4] Young Researchers and Elite Club, Delvar Branch, Islamic Azad University, Delvar, Iran. Mehdi.gheisari61@gmail.com

2-1-3 Sinkhole Attack

This types of attack that are the specific attacks of the wireless sensor networks, a malicious node equipped with the powerful hardware, is placed with in the network that approximately is connected to the whole part of the network or placed near the sink node. And immediately after the receiving the data, they will be diverted to another route out of the network. This type of attacks caused the Selective Forwarding Attacks and Wormhole Attacks are created.

2-1-4 Sybil Attack

Sometimes we need to use of the identifier (ID) in designing of network topology and routing that are given by given this unique ID. In this type of attacks, the malicious nodes is placed within the network and it offers the number of ID's and actually it indeed goes over the network nodes. This will affect the causing to the geographically routing problems, distributed storage, multidirectional routing and changing the topology.

2-1-5 Wormhole Attack

This attack is preferred by multiple malicious nodes that are located in two different spots in the network. The connection between this two nodes is a faster connection. The source node received the data from networks and sends them to the destination node.

III. Attack avoiding approaches

Using the shared key and the encrypted data - to avoiding external attacks such as Sybil Attack and Selective Forwarding

Assigning the unique key to the nodes and also restricting the neighbors' nodes to prevent Sybil Attacks.

Careful designing of the routing protocol and using the geographical routing to avoiding Wormhole and Sinkhole attacks.

Multi-directional routing and ensuring the neighbor nodes to avoid the Selective Forwarding attacks.

IV. Conclusion

Wireless sensor networks have introduced us the new class of telecommunications networks. These networks are enabling us to understanding that what's happening in the physical environment that is even possible human presence there. For example, to study the behavior of nature, wild animals escape is caused by the presence of any sensor is essential. In general the sensor networks for their high speed data transmissions and low costs, low volume have the significant impacts on financial security, life and health care. In the healthcare monitoring, sensor network applications reduces costs of individuals and increase the speed of response in emergency situations. Sensor networks give vast perspectives to us to creating a variety of applications to improve the lives and communities deal. Monitoring the stores to prevent theft, monitoring roads to controlling the traffic and prevent road accidents and subtle care of elder people in this category are applied. Furthermore, sensor networks can have been in the near future an important role in the development of a new generation of equipment, weapons and armors.

References

[1]S. S. Camtepe and B. Yener. Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks.IEEE/ACM Transactions on Networking , 15(2):346–358, 2007. http://dx.doi.org/10.1109/TNET.2007.892879

[2]D. Chakrabarti, S. Maitra, and B. Roy. A Key Pre-distribution Scheme for Wireless Sensor Networks: Merging Blocks in Combinatorial Design. In Information Security , pages 89–103. LNCS 3650, 2005.

[3]H. Chan and A. Perrig. Security and privacy in sensor networks.Computer, 36(10):103–105, 2003. http://dx.doi.org/10.1109/MC.2003.1236475

[4]H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor net-works. In Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy, 2003 IEEE Symposium on Security And Privacy, pages 197–213, Berkeley, CA, United States, 2003. Institute of Electrical and Electronics Engineers Inc.

[5]W. Y. Chang. Wireless Sensor Networks and Applications. In Network-Centric Service- Oriented Enterprise, pages 157–209. 2008.

[6]H. Choi, S. Zhu, and T. F. La Porta. SET: Detecting node clones in sensor networks. In Third International Conference on Security and Privacy in Communications Networks and the Workshops (SecureComm 2007) , pages 341–350, 2007.

[7]J. Y. Chun, Y. H. Kim, J. Lim, and D. H. Lee. Location-aware Random Pair-wise Keys Scheme forWireless Sensor Networks. In Third International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SECPerU 2007) , pages 31– 36, 2007. http://dx.doi.org/10.1109/SECPERU.2007.7

[8]J. Deng, R. Han, and S. Mishra. INSENS: Intrusion-**Tolerant** Routing in Wireless Sensor Networks. Technical Report Technical Report CU-CS-939-02, University of Colorado, Department of Computer Science, 2003.