Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 6, June 2015, pg.654 – 657

RESEARCH ARTICLE

A Study on Different Attacks in WSN

Ritu

R.N College of Engg. & Management, Rohtak (Haryana)

Ritu4648@gmail.com

Pooja Ahlawat

Asstt. Prof, CSE Deptt., R.N. College of Engineering and Management, Rohtak

Pooja.ahlawat5@gmail.com

Abstract: Security is one of the most crucial and adaptive requirement for any network. When the network is defined under energy restriction, the criticality of network increases. In this paper, a study on different aspects of sensor network are defined. The paper has discussed the WSN under security requirement and associated threats. The paper has discussed some of the common attacks in sensor network.

I. Introduction-

Wireless Sensor Network are spatially distributed autonomous sensors to monitor physical or environmental condition and to cooperatively pass their data through the network to a main location[5]. The WSN is built of “nodes”- from a few to several hundreds or even thousands, where each node is connected to one or sometimes several sensors. In order to extend the sensor network lifetime, the efficient use of energy becomes the focus of the study of WSN.

Research on WSN includes routing technology, positioning technology, and energy control and security assurances. Jamming attacks effects the WSN mostly at physical and MAC layer[1]. Jamming attack reduces the performance by unnecessary use of resources. The technology of the WSN can be applied to many situations. It could be used to observe environmental pollution, prevention of forest fires, cultivating crop, supervision of poisonous chemicals, and even monitor the enemy in a war[6].

Jamming is the type of attack which interferes with the radio frequencies used by network node. Jamming attack may be viewed as a special case of Denial Of Service attacks[1]. In a jamming attack the radio frequency signal emitted by the jammer corresponds to the “useless” information required by all sensor nodes. This signal can be white noise or any signal that resembles network traffic.

Each kind of jammer behaves in different ways in different monitoring mechanism(Continuous monitoring and Periodic monitoring). The important objective of paper is to find the Nash equilibrium condition for players and to propose the efficient detection mechanism against all kind of jamming[1]. The proposed detection mechanism uses clustering of cross layer features for efficient detection of jamming. The approach helps to easily detect the normal and abnormal behavior in game, and to inform the network to take the particular action against jamming attack. The presented work will be able to generate the effective and reliable communication route over the wormhole infected communication network. The work will identify the jamming attack as well generate the preventive path over the network. The behaviour specific modelling will reduce the efforts for attack detection over the network. The analysis of work will be defined in terms of throughput, lossrate and response time parameters[3,4].

II. Related Work-

Game theory offers various ways to formulate the problems posed by malicious nodes; it can also work in analyzing WSN security attacks. Malicious nodes in security related games within the network can launch an active attack on other nodes, where malicious nodes will disrupt network operation. Now we will define the attacks related to game theoretic approaches[1].

- When external intruder attack is most vulnerable node in the network then the defense strategy is “IDS protects the cluster of nodes from the intruder”, the ideal strategy is “IDS protects the same cluster which intruder attacks” and payoff function is “function of utility, cost of defending/ protecting a cluster”.
- When external intruder injects malicious packet in the network then the defense strategy is “service provider tries to detect malicious packets by sampling network flows at various links”, the ideal strategy is “sampling strategy should be greater than the maximum flow of packets” and payoff function is “function of probability for detecting a malicious packet”.
- When external attacker causes nodes to turn malicious by causing them to prevent broadcast messages from reaching other nodes then the defense strategy is “a certain subset of nodes, unknown to attackers sends acknowledgement to the base station for the broadcast messages”, the ideal strategy is “detect attacked nodes so that attacker payoff goes to zero” and payoff function is “attacker payoff is proportional to the number of nodes deprived of the broadcast messages”.
- When internal intruder is malicious nodes do not forward incoming packets then the defense strategy is “introduce reputation ratings for collaboration between nodes”, the ideal strategy is “catch nodes in the process of being malicious, i.e. while dropping packets and payoff function is “Function of a discount factor times the previous payoff”.
- When internal attacker is malicious nodes in mobile WSNs do not forward incoming packets then defense strategy is “ maintain good cooperation, reputation and quality of security ratings at each node” , the ideal strategy is “nodes cooperate only if there has been a good history of cooperation and payoff function is “function of the distance between nodes, number of packets forwarded and received”.

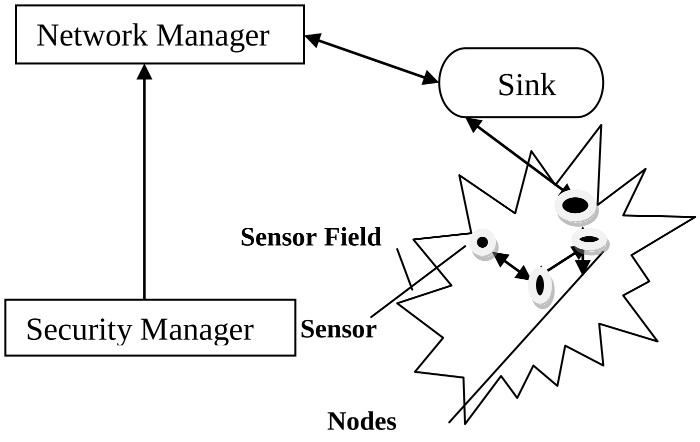

Figure 1 Architecture of Wireless Sensor Network

Various Jamming Attacks-

- Deceptive Jammer: The deceptive jammer sends the packet continuously without checking for channel. During continuous monitoring Df can gain the G" and G" alternatively by paying the cost Pdj or Pc respectively. In periodic monitoring, the DJ can gain G" by paying cost P"j' while it can gain G" by paying Pp after some period t.
- Random Jammer: The random jammer uses the combine strategies of constant jammer and deceptive jammer. The different strategies of random jammer are as shown in table.
- Reactive Jammer: The reactive jammer reacts only when it senses any event on the channel. In continuous monitoring, reactive jammer can achieve the gain G" by paying cost Prej during attack duration AD, otherwise it gain Gd by paying cost of continuous monitoring Pc. During periodic monitoring, the Ref can gain G" with period t by paying Prej in every attack duration AD, else it can gain G" in every AD by paying Pp after period t.

III. Security-

Wireless sensor nodes network means that shares common property as computer network. So we need security issues: - 1Attack and Attacker: - Attack means that unauthorized person access to a service. For security we need secure resource or information we need integrity, availability, or confidentiality of a system. Attackers can create fault and weakness in a security design, implementation, configuration or limitation are occurs[2,7,8].

- Authentication:-WSNs transfer information and sensitive data for different important decision making. Receiver wants to the data with ensure that are correct source for decision-making process. Authentication provides proof to sender node and receiver that data is secure in which they want to communicate.
- Integrity:-Integrity means ensure that there must no tampering and extra data. Receiver check that data received is exactly original and same as send by the sender. Data integrity is to ensure that information is same during transmission by using some security key for ensure.
- Confidentiality:-It gives guarantee that data send by the sender will not access by attacker. Encryption key is used for sending the message. Confidentiality means create security from unauthorized parties and attacker.
- Scalability:-Scalability means that no node compromise and no increase communication when size of network is grow. It should allow nodes to be added in network with proper deployment as well.
- Self-Organization:- In WSN Every sensor node is in dependent and flexible enough to be self organizing in different environments. No fixed infrastructure is available for WSN Network management. In self organizing we used conduct key management. In self organization we used conduct key management and building trust relation among sensor for security.

Host Based Vs Network Based-

During compromising users of WSN:- By cheating user share information like as password or keys about the sensor nodes. Two types compromise hardware and software. In hardware involve tempering with the hardware to extract the programming code and data and keep store with in sensor node. In software compromise involve breaking the software running on sensor node.Network attacks compromise old on layer specific and protocol specific. In this, attacker's purpose not disturbs the service availability, message confidentiality and security but gain an unfair advantage for itself in the usage of network.

WORMHOLE ATTACK:-Wormhole attack like as a denial of service attack that disturb the network communication infrastructure without knowledge of the cryptography key methods. In wormhole attack may be created by a single or a pair of collaborating nodes in which two or more attackers are connecting by high speed off-channel link called wormhole link. A wormhole attack could be launched in two different modes: hidden and participation mode. In wormhole attack modes are depending upon attackers add their identity into packet headers when tunneling and replaying messages. In hidden mode attackers are not seen by the legitimate nodes. In this mode attackers put him on powerful position and during transmission capture message at one end of the wormhole and replicate them at the another end. This mode not need information about the authentication and encryption because its purpose only disturb and confused routing mechanisms. In this way it can create a virtual link between two far-off nodes by for example “tunneling“the hello messages. So that hidden-mode wormhole attack is more difficult to defend against it. In participation mode attackers acquire valid cryptographic keys to attack on legitimate nodes. In this mode an attacker no need to create virtual link between the legitimate nodes.

IV. Conclusion

The paper has discussed some of the common security issues in sensor network. The also identified the criticalities in the network and the security threats in the network itself. The paper discussed the associated network attacks applied by internal or external nodes.

REFERENCES

[1] Sachin D.Babar, Neeli R. Prasad, Ramjee Center for TeleInFrastruktur, Aalborg University Aalborg, Denmark {sdp,np,Prasad}@esaau.dk

[2] Debashis De, Aditi Sen, Madhuparna Das Gupta Department of Computer Science & Engineering BF-142, Sector 1, Salt Lake City, West Bengal University of Technology, Kolkata 700064, West Bengal, India

[3] Anbang Zhao, Cheng He, Bin Zhou College Of Underwater Acoustic Engineering Harbin Engineering University Harbin, China hecheng@hrbeu.deu.cn

[4] Chow-Sing Lin∗, Chih-Chung Chen† and An-Chi Chen‡ ∗*Dept. of Computer Science and Information Engineering National University of Tainan Tainan, Taiwan (R.O.C.) 700 Email:mikelin@mail.nutn.edu.tw*

[5] Yankun Li, Ming Zhu School of Business Administration Changchun University of Technology Changchun, P.R.China Yiyi9999yiyi@yahoo.com.cn

[6] Jacqueline Stewart, Robert Stewart, MN Hassan Dept. of Electronics, Computer and Software Engineering, The Wireless Networking Group, Athlone Institute of Technology, Athlone, Co. Westmeath, Ireland. {jstewart; nhassan } @research.ait.ie rstewart@ait.ie

[7] Anbang Zhao, Cheng He, Bin Zhou College of Underwater Acoustic Engineering Harbin Engineering University Harbin, China hecheng@hrbeu.deu.cn

[8] Jian Guan1,2, Xuejie Liu1, Xinhua Lu1, Yanheng Liu1
1. College of Computer Science and Technology, Jilin University
2. College of Information Communication Engineering, Changchun University of Technology Changchun, China guanjian.jlu@gmail.com

[9] Zheng Gengsheng School of Computer Science & Engineering Wuhan Institute of Technology Wuhan 430073, China e-mail: zhenggengsheng@sina.com

[10] Mohammad Mehdi Shirmohammadi#1, Karim Faez *2, Mostafa Chhardoli#3 # *Islamic Azad University hamedan branch, Hamedan, Iran* 1,3*{mmshirmohammadi,chhardoli}@gmail.com * EE department of Amirkabir University of Technology, Tehran,Iran 2kfaez@aut.ac.ir*

[11] Mingyan Li, IordanisKoutsopoulos, Radha Poovendran, "Optimal Jamming Attacks and Network Defense Policies in Wireless Sensor Networks", IEEE Transaction on Mobile Computing, Vol. 9, Issue S, pp.1119-1133, 2010.