Security Architecture for Attack of Malicious Signals in Wireless Network

Bimal Kumar Mishra, Santosh Kumar Srivastava, Rama Kant Mishra, Binay Kumar Mishra

***Abstract*— In this architecture, sensor field is divided into clusters and there are two types of nodes i.e. high end gateway node and regular node .Regular nodes are inexpensive to make the network cost effective. Gateway nodes monitor the regular nodes. Honeypot node monitored gateway node. Base station controlled and monitored honeypot node. With this a honeynet is formed, which can defend against Attacks.**

***Index Terms*— Honeypot, gateway, worms.**

I. INTRODUCTION

Wireless Sensor Network is composed of thousands of self-powered tiny sensor nodes which gather information or detect special events and communicate via radio transmitter or receivers, with the end goal of handing their partially processed data to the base station. Sensing, processing and communication in one tiny device gives rise to a vast number of applications such as environmental monitoring, target tracking, home applications, monitoring disaster area, vehicle tracking etc [1]. Wireless network is prone to attacks in every layer [2-4] as shown in Table 1, as a result many defense mechanism has been developed .The defending approach against hello flood attack is discussed in [5] . In [6] ,security mechanism to defend against the Sybil attack. In [7] , defend mechanism against wormhole attack in wireless network. In [8] authors discuss the defense scheme against DOSs. These security techniques are not perfect solutions where network is prepared to defend against specific types of attacks.

In real world we cannot know what type of attack will launch, moreover there are one or several attacks by an attacker or there may be several attackers in different area of the network targeting different nodes by using different attacks. To provide defense for all known attack at different layer is not possible with low memory end sensor nodes and using only high end sensor nodes presents cost constraint. The security scheme must be able to defend against all known as well as unknown attacks at any given time without presenting cost constraint. Major obstacle in employing an efficient security scheme comes from the resource starved nature of WSNs like low memory and processing power, limited battery life and bandwidth, and easy accessibility of wireless channels by good citizens and attackers. Worms are easy to write program and payload is independent of propagation which distinguishes it from conventional attacker tools, and which lends a very fast growth [9]. In order to defend the WSN against all aforementioned attacks we need automatic responses because of the speed of worms. Use of IDS (intrusion detection system) for WSN[10-15], many surveys have been published for anomaly detection but none of them tackle the problem of intrusion detection in specific. Existing IDS are not adequate to protect WSN. According to [4] there is no intrusion detection model specific for WSN like other type of network. We need a robust security framework which must be able to automatic detect attacks and respond against attacks and discover new attacks. In this paper we divide our work in four parts Prevent, detect, defend and discover mechanisms. We have considered prevent mechanism where Encryption and authentication protocol are applied as a first line of defense to prevent outsiders attacks, however some attacks like sinkhole, wormhole etc could not be detected using this kind of preventive mechanism. When prevention mechanism fails, we have to detect such attacks and respond against them. One possible detector is a "Honeypot", which capture and analyze the behavior of attackers.

It is highly sensitive to worm activity as well as other known/unknown attacks [16-18]. In addition to detection, we‟ve also been considering defend mechanisms. In order to defend against attack we switch the compromised sensor nodes to sleep state and run the defending scheme against the detected attacks. In sleep state sensor node does not communicate with other nodes or does not participate in routing process, so in sleep state it is not able to spread attacks, but the nodes are able to process the data in sleep state [1]. This mechanism also conserves energy in sensor network. We also consider the discover mechanisms for new unknown attacks. In traditional security approach where network is prepared to defend against specific attack does not work in reality. One cannot know what type of attack adversary will launch. Combining many defends mechanism and making them work in collaboration is not possible with memory constraint inexpensive sensor nodes. Therefore, we propose to develop a framework that can provide this capability. In this paper, we propose security architecture for sensor network where there is a combination of low-end sensor nodes along with high-end sensor nodes and honeypot. Our contribution in this paper is the combination of several techniques and the creation of new defend mechanism, based on these techniques.

Bimal Kumar Mishra, Department of Applied Mathematics, Birla Institute of Technology Mesra, Ranchi, India
Santosh Kumar Srivastava, Department of Computer Applications, Vinoba Bhave University, Hazaribag, India
Rama Kant Mishra, Department of Physics ,Hindustan College of Science and Technology, Farah Mthura, India
Binay Kumar Mishra, Department of Physics, Maharaja College, Veer Kunwar Singh University, Ara, India

Physical Layer Attack	Jamming, Tampering attacks
Data Link Layer attack	Collision, Exhaustion, Unfairness attacks
Network Layer Attack	Spoofing, Selective Forwarding, Sinkhole, Sybil, Wormhole attack, Hello Flood attack, Acknowledgement spoofing attacks
Transport Layer Attack	Flooding and desynchronization attacks

Table 1

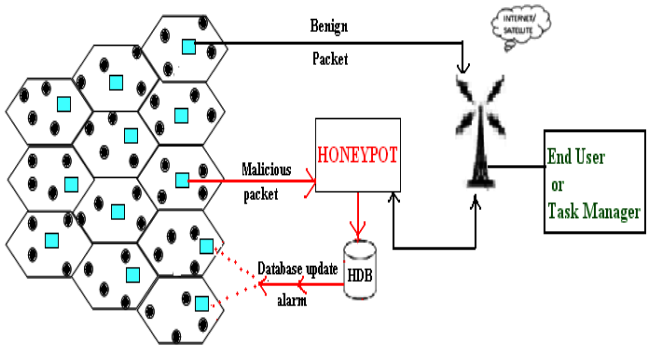

Figure:1

In Figure 1, a cluster-based detection approach for WSNs is proposed. In this approach, a network is divided into clusters (like GSM cells), clustering is done to save energy in sensor network [22]. Suppose we have 10,000 regular sensor nodes spread in a vast area and 25 clusters are formed, each cluster consists of 400 regular nodes and a gateway node. So there will be total of 25 gateway nodes in the network. Since the Gateway monitors its cluster‟s nodes, so the overall network energy cost is reduced because not all the sensor nodes keep monitoring. Each Gateway node consist of "detect and defend" database, in which there is a set of attacks A={A1, A2,…An} consisting of n number of attacks. For any attack Ai there is a defense mechanism D={D1, D2….Dn} and for each defense mechanism Di, the program size is Pi . Since memory capacity is not concern with gateway nodes, we assume to have "detect and defend" database are available on each gateway node to detect all the known attack in its cluster. The gateway nodes may also detect attacks against the other neighbor gateway nodes of the network, as they constitute the backbone of the routing infrastructure. Each gateway node is then monitored by a Honeypot node. When the gateway node is unable to defend the attacks, the packet is redirected to "Honeypot node" where the behavior of attacks is captured and new discovered attack is stored in Honeypot database (HDB) and "detect and defend" database of gateway node is updated according to honeypot database(HDB). In turn, Honeypot nodes will be controlled and monitored by the Base station. Base station is much more powerful node with large storage, all the database; detection rules are stored primarily as backup in base station. This backup system increases the reliability of the whole network.

Conclusion

In this paper, we try to design an efficient security framework for Wireless network. The major obstacle in designing efficient security architecture comes from resource constraint nature of WSN. Our proposed architecture "Prevent Detect and Defend mechanism for Wireless network using Honeynet" is energy efficient as well as cost efficient and able to detect known/unknown attacks. In this architecture few expensive Gateway nodes are deployed which is responsible for monitoring its cluster member, so the overall network energy cost is reduced because all the sensor nodes need not be keep monitoring. We are also preventing the spread of attacks by switching the infected nodes to sleep state, this mechanism also conserve energy. The Honeypot is efficient tool in contrast to firewall, IDS and other security technologies because of high efficiency to capture data, low miss alarm and false alarm, low price of the deployment and it can detect known/unknown attacks and worms.

REFERENCES:

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, *"Wireless sensor networks: a survey"*,Computer Networks, 38:393-422, 2002.

[2] Shio Kumar Singh, M P Singh, and D K Singh,*"A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks"*, International Journal of Computer Trends and Technology- May to June Issue, 2011

[3] A. Pathan, H.-W. Lee, and C. S. Hong,*"Security in wireless sensor networks: issues and challenges,"* in *Proceedings of the 8th International Conference Advanced Communication Technology*, vol. 2, February 2006, pp. 1043–1048.

[4] Murad A. Rassam, M.A. Maarof and Anazida Zainal , *"A Survey of Intrusion Detection Schemes in Wireless Sensor Networks"*, American Journal of Applied Sciences 9 (10): 1636-1652, 2012 ISSN 1546-9239, © 2012Science Publication.

[5] M. A. Hamid, M. Mamun-Or-Rashid, and C. S.Hong, *"Routing security in sensor network:Hello flood attack and defense,"* in *Proceedingsof 1st International Conference on NextGeneration Wireless Systems*, January 2006, 52–56.

[6] J. Newsome, E. Shi, D. Song, and A. Perrig,*"The sybil attack in sensor networks:analysis &defenses"*, Proc. of the third international symposium on Information processing in sensor networks, ACM, 2004, 259 - 268.

[7] Y.-C. Hu, A. Perrig, and D. B. Johnson, *Packetleashes: A defense against wormhole attacks in wireless networks*, in Proc of IEEE Infocomm 2003,

[8] A. Wood and J. Stankovic, *"Denial of service insensor networks"*, IEEE Computer, pages 5462, Oct. 2002.

[9] SANS Institute 2004, SANS Institute InfoSec Reading Room, *"Worm Propagation and Countermeasures'*.

[10] OTran Hoang Hai, Faraz Khan, and Eui-Nam Huh, *"Hybrid Intrusion Detection System for Wireless Sensor Network"*, ICCSA 2007, LNCS 4706, Part II, 383–396, 2007. Springer-Verlag Berlin Heidelberg 2007

[11] Rodrigo Roman, Jianying Zhou , Javier Lopez, "*Applying Intrusion Detection Systems to wireless sensor networks "*,Consumer Communications and Networking Conference, 2006. CCNC 2006. 3rd IEEE, 8-10 Jan. 2006 Volume: 1, 640- 644, ISBN: 1-4244-00856

[12] C.-C. Su, K.-M. Chang, Y.-H. Kuo, and M.- F. Horng, *"The new intrusion prevention and detection approaches for clustering-based sensor networks"* ,in 2005 IEEE Wireless Communications and Networking Conference, WCNC 2005: Broadband Wirelss for the Masses - Ready for Take-off, Mar 13-17 2005.

[13] Djallel Eddine Boubiche and Azeddine Bilami, *"Cross Layer Intrusion Detection System For Wireless Sensor Network"*, International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012.

[14] Mohammad Saiful Islam Mamun, A.F.M. Sultanul Kabir, *"Hierarchical Design Based Intrusion Detection System For Wireless Ad Hoc Sensor Network"*, International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.3, July 2010.

[15] Dmitriy Martynov, Jason Roman, Samir Vaidya, and Huirong Fu, *Member, IEEE, "Design and Implementation of an Intrusion Detection.*