INTRUSION DETECTION SYSTEM FOR WSN: A REVIEW

Umesh Gupta[1], Gulshan Soni[2], Nikhil Singh[3]
[1,2]*ME Student, NITTTR, Chandigarh*
[1]er.umeshgupta@gmail.com
[2]gsoni260@gmail.com
[3]*M.TechStudent, AMU, Aligarh*
[3]nikhil26194@gmail.com

***Abstract*: Secure Network Communication plays a vital role in the development of modern world. With the rapid growth of wireless sensor network that is vulnerable to a wide range of attacks due to deployment in the hostile environment and having limited resources. The main target of attackers is network system which is increasing day by day. Intrusion detection system is one of the major and efficient defensive methods against attacks in WSN. In this paper, an introduction and brief review of some recent intrusion detection system in WSN, which will helps to researcher.**

***Keyword*- Intrusion Detection System, Wireless Sensor Network, Attacks,**

I. INTRODUCTION

Wireless Sensor Network

Wireless Sensor Networks (WSN) consists of small devices—called sensor nodes—with RF radio, processor, memory, battery and sensor hardware. One can precisely and deeply monitor the environment with widespread deployment of these devices. Sensor nodes are resource-constrained in terms of the radio range, processor speed, memory size and power. WSN follow specific communication patterns. Apart from this, sensor nodes are generally stationary. The traffic rate is very low and generally the traffic is periodic as well. There may be long idle periods during which sensor nodes turn off their radio to save energy consumed by idle listening. Recharging or replacing batteries is expensive and may not even be feasible in some situations. Therefore, WSN applications need to be extremely energy-aware.
WSN is mostly unguarded. Hence, capturing a node physically, altering its code and getting private information like cryptographic keys is easily possible for an attacker. Wireless medium is inherently broadcast in nature.
This makes them more vulnerable to attacks. Attacks can disrupt the operation of WSN and can even defeat the purpose of their deployment. An adversary can launch DoS attacks without effort.

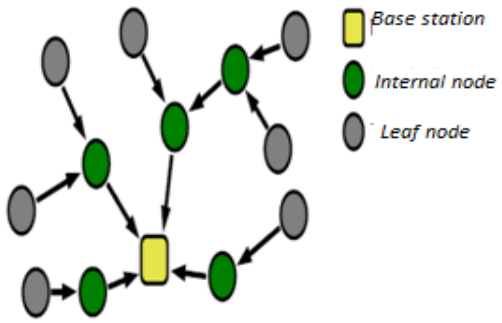

Fig1. Wireless Sensor Network

Wireless Sensor network can be categorized in two parts:

- *Homogenous WSN:* A homogeneous sensor network consists of identical nodes.
- *Heterogeneous WSN:* A heterogeneous sensor network consists of two or more types of nodes.

Intrusion

The term intrusion means both intrusion by outsider and insider abuse.
There are several classical security methodologies so far that focus on trying to prevent these intrusions. A lot of work in sensor network security has focused on particular types of attacks and how they can be prevented. This can, however, only be a first line of defence. It is impossible, or even infeasible, to guarantee perfect prevention. Not all types of attacks are known and new ones appear constantly. As a result, attackers can always find security holes to exploit. For certain environments it makes sense to establish a second line of defence: An Intrusion Detection System (IDS) that can detect an attack and warn the sensors and the operator about it.
It categorized intrusions into three types:

- *Misuse or Signature-based detection:* Intruder takes advantage of weaknesses in

the system and finds out a way to get in. We can formally define these attack patterns. These attack patterns are called as signatures. So if new adversary tries to use known attacks to intrude then he will be caught if his pattern of attack matches some signature.

- *Anomaly detection:* In this type of intrusion detection, normal user behaviour is defined and the intrusion detection system looks for anything that is anomalous hence suspicious. Anomaly detection assumes that intrusion is a kind of anomalous activity. So if it detects anomalous behaviour, it can detect an intrusion.

- *Specification-based Detection System:* Specification-based detection system works by defining rules for attacks. Sensor node's behaviour is checked against each rule sequentially. There is a failure bit associated with each node. If the sensor node violates any rule, failure bit is incremented. If number of failures of a particular node increases than a threshold after a time interval t; an alert about that node is generated.

II. TYPES OF ATTACKS

There are many types of attacks they are able to perform. We focus on active external and internal attackers (insiders) as they are able to run more convenient attacks and the intrusion detection system is deployed to defend against these attack .IDS is used to differentiate among trusted nodes and attackers as they might form a legitimate part of the network symptoms of attacks are very important for the study of intrusion detection systems for WSN. IDS may determine an internal attacker in the network based on the pre-defined symptoms of known attacks.

1) Active Attacks

These are such types of attacks in which the attacker cause destruction. There is physical damage in the network like destruction of resources, alteration of data, changing traffic direction or stoppage of data to sink nodes. These attacks are easily identifiable and we can stop the attackers as well as start the system recovery process.

2) Passive Attacks

These are another types of attacks in which the attackers only observe different activities on the network check confidential information but don't cause any physical destruction or any alteration of information. However the passive attackers can launch active attacks and cause a big damage because during observation of different activities on the network he is able to find weak points and clues in the network and wait for a suitable time to launch an attack. Passive attacks are more dangerous as compare to active attacks because in passive attacks you are unable to recognize your attacker.

3) Jamming attack

Jamming is interfering with the radio frequency used by nodes for their communication. It is performed by deliberate transmission of radio signals. It is used to conduct a denial of service attack as nodes cannot communicate at all while a jamming attack is ongoing. Among the ones that may be the most effective are constant, deceptive, random and reactive jammers.

A *constant jammer* continually emits a radio signal without respecting any medium access protocol. In this case, other nodes never find the medium idle. A *deceptive jammer* uniformly injects regular packets without any gap so other nodes stay in the receiving mode most of the time. A *random jammer* emits or is asleep to reduce battery consumption. It switches these two states in a random manner. Random jamming may be implemented by both constant and deceptive jammers. A *reactive jammer* emits only when there is communication on the medium.

4) Hello flood attack

Routing protocols usually prefer the shortest or the most reliable path to the base station. Hello packets (sometimes also referred to as advertisements or beacons) are sent out by a new node in the network in order to inform other nodes that they can possibly route their messages via the new node. If a malicious node possesses a long-range antenna, it can broadcast hello packets claiming good connection to the base station. These hello packets will be received by the nodes which cannot reach the adversary back as they do not have such a strong antenna.

5) Selective forwarding

A compromised node (an attacker) drops packets instead of forwarding them further in a Multi-hop routing system in case of a selective forwarding

attack. An attacker may drop all of the incoming packets (also denoted as *black hole attack*) or selectively drop only specific packets (coming from a specific source, having a certain destination, containing certain payload data, etc.). In the second case, it is harder to detect and several statistics have to be stored by an IDS to check.

6) Sinkhole attack

A sinkhole node is one where most of the traffic is reflected. According to a routing protocol, it is the one claiming extremely good connection to the base station in its neighbourhood. An attacker tries to create a sinkhole node from the one that is captured by them. Afterwards, more serious attacks can be run using this node. Depending on which routing algorithm is used, an attacker tries to fake routing protocol's metrics which define the best path to the gateway so most of its neighbours, preferably all, set the captured node as their parent node.

7) Packet alteration

An attacker might be interested in spoofing or altering packets of other nodes in order to misuse a routing algorithm have an advantage in voting protocols or change measured values sent by sensor nodes to the base station. The basic assumption is that a node should be able to hear only packets that have originated in its neighbourhood. If they have originated elsewhere, they are spoofed packets. So packet alteration is one of the major vulnerable attacks in intrusion detection system for wireless sensor network.

8) Denial of service Attack (DoS)

The main objective of this attack is to waste the available resources of the network. In this attack the attacker (malicious node) send extra packets in the network without any need and keep the route as well as the base station busy. So the authentic users are unable to send data, access resources and get services. Therefore DoS attack is launched to prevent the legitimate users of the network from utilization of resources to get any service. DoS attack may vary from layer to layer in OSI model. At physical layer DoS attack may be in the form of traffic blockage and delay, at data link layer it may cause collision of frames and unfairness. DoS attack at network layer may be packet routing in wrong direction as well as black holes creation. While on transport layer DoS attack may be flooding (extra traffic) or resynchronization of data in the network [2].

9) Worm holes

In this attack the whole traffic of the network is tunnelled in a particular direction at a distant place, which causes deprivation of data receiving in other parts of the network. Sometime any information which is very important and should be delivering to the base station in specific time which is sends toward worm hole [3].

10) Looping

In this attack few nodes in the network cause the circulation of data in a particular region. This attack stops data to send to a destination node and revolve in the same region which increase network traffic as well as causes latency [3].

IV. COMPARATIVE ANALYSIS OF RECENT INTRUSION DETECTION SYSTEM SCHEMES

The comparative analysis of recent IDS has been discussed in TABLE I.

V. CONCLUSION

In this paper, we present a brief review of recent attacks and recent works on different approach of IDS for wireless Sensor Network. As, we all know that intruder detection system is essential part of security for every network. WSN are vulnerable to a number of internal attacks and external attacks that affects the overall performance of the network. These attacks results in wrong interpretation of the sensor field. The need of the day is an IDS for detecting intrusion accurately in an energy-efficient manner. So, we can say that scope for future is to make one IDS which utilizes less resource (energy) and provide better security. This paper helps to make an efficient Intruder detector system.

REFERENCES

[1] http://www.krazytech.com/technical-papers/computer-science-technical-papers-technical-papers/security-requirements-in-wireless-sensor-networks (accessed on 14 May 2012).

[2] Mona sharifnejad, Mohsen Sharifi, Mansoureh Ghiasabdai, S. Beheshti, "A Survey on Wireless Sensor Networks Security", Proceeding of International Conference Science of Electronics, Technologies of Information and Telecommunication, pp. 25-29, March 2007.

[3] B. Parno, A. Perrig, V. Gligor, "Distributed Detection of Node Replication Attacks in Sensor Networks", Proceeding of IEEE Symposium on Security and Privacy, pp.210-218,May 2005.

[4] B.J. Culpepper, H.C. Tseng, "Sink hole intrusion indicators in DSR MANET's" Proceeding of International Conference on Broad Band Networks,pp.681-688, May 2004.

[5] Blackrert, W.J. Gregg, D.M. Castner, A. k. Kyle, E.M. Home, "Analyzing Interaction between

Distributed Denial of service Attacks and Mitigation Technologies" Proceeding of International Conference on information Survivability and Exposition, DARPA, pp. 26- 36, April 2003.
[6] T. Bhattasali, R. Chaki, "A Survey of Recent Intrusion Detection Systems for Wireless Sensor Network" Proceedings of Fourth International Conference on Network Security and Applications (CNSA 2011), pp. 268-280, July 2011.
[7] Yuxin Mao, "A Semantic-based Intrusion Detection Framework for Wireless Sensor Network", Proceeding of sixth International Conference on Networked Computing (INC),pp. 28-36, June 2010.
[8] Sudip Misra, P. Venkata Krishna and Kiran Isaac Abraham, "Energy Efficient Learning Solution for Intrusion Detection in Wireless Sensor Networks", Proceedings of the 2nd international conference on Communication systems and Networks, pp. 36-42, September 2010.
[9] Garth V. Crosby, Lance Hester, and Niki Pissinou, "Location-aware, Trust-based Detection and Isolation of Compromised Nodes in Wireless Sensor Networks", Proceeding of International Journal of Network Security, pp.107- 117,March 2011.
[10] Rung-Ching Chen, Chia-Fen Hsieh and Yung-Fa Huang, "An Isolation Intrusion Detection System for Hierarchical Wireless Sensor Network", Proceeding of Journal of Networks, pp.29-37, March 2010.
[11] Rung-Ching Chen, Yung-Fa Huang, Chia-Fen Hsieh, "Ranger Intrusion Detection System for Wireless Sensor Networks with Sybil Attack Based on Ontology", Proceeding of New Aspects of Applied Informatics, Biomedical Electronics and Informatics and Communications ,pp. 219-227, April 2010.
[12] Mohammad Saiful Islam Mamun, A.F.M. Sultanul Kabir, "Hierarchical Design Based Intrusion Detection System For Wireless Ad Hoc Sensor Network", Proceeding of International Journal of Network Security & Its Applications (IJNSA), pp. 113-121, July 2010.
[13] K.Q. Yan, S.C. Wang, C.W. Liu, "A Hybrid Intrusion Detection System of Cluster-based Wireless Sensor Networks", Proceedings of the International Multi Conference of Engineers and Computer Scientists, pp. 67-71, March 2009.
[14] Idris M. Atakli , Hongbing Hu, Yu Chen, Wei-Shinn Ku, Zhou Su "Malicious Node Detection in Wireless Sensor Networks using Weighted Trust Evaluation", The Symposium on Simulation of Systems Security (SSSS'08) ,April 2008
[15] Guangcheng Huo, Xiaodong Wang, "DIDS: A Dynamic Model of Intrusion Detection System in Wireless Sensor Networks", IEEE, International Conference on Information and Automation, pp. 56-64, June 2008.
[16] A.H. Farooqi, F.A. Khan, "Intrusion Detection Systems for Wireless Sensor Networks: A Survey", Proceeding of Communication and Networking International Conference, FGCN/ACN, pp. 234-241,December 2009.
[17] Chun-ming Rong , Skjalg Eggen , Hong-bing Cheng, "A Novel Intrusion Detection Algorithm for Wireless Sensor networks" Proceeding of 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology (Wireless VITAE), pp. 1 – 7 , March 2011.
[18] Meijuan Gao, Kai Li, Jingwen Tian, " Wireless Sensor Network for Community Intrusion Detection System based on Embedded System" Proceeding of Control and Decision Conference, pp. 4696 - 4699 , July 2008.
[19] Yang Liu and Fengqi Yu," Immunity-Based Intrusion Detection for Wireless Sensor Networks" Proceeding of IEEE International Joint Conference on Neural Networks, pp. 439 - 444, June 2008.
[20] S.V.Patel, Kamlendu Pandey and Dr V R Rathod , "A Decentralised Clustered and Hash based Intrusion Detection System for Wireless Sensor Networks" Proceeding of Fourth International Conference on Wireless Communication and Sensor Networks, pp. 27 - 30 , December 2008.
[21] Mounib Khanafer, Mouhcine Guennoun, Hussein T. Mouftah, "Intrusion Detection System for WSN-based Intelligent Transportation Systems" Proceeding of IEEE Global Telecommunications Conference, pp. 1 - 6 , December 2010.
[22] M. Poorani, V. Vaidehi, M. Rajesh, Bharghavi, Mr. Balamuralidhar and Dr.Girish Chandra, "Semantic Intruder Detection System in WSN" Proceeding of second International Conference on Advanced Computing (ICoAC), pp. 26 - 32 , December 2010.
[23] Abror Abduvaliyev, Sungyoung Lee, Young-Koo Lee, "Energy Efficient Hybrid Intrusion Detection System for Wireless Sensor Networks" Proceeding of International Conference On Electronics and Information Engineering (ICEIE), pp. V2-25 - V2-29 , August 2010.
[24] Zhenwei Yu, Jeffrey J.P. Tsai,"A Framework of Machine Learning Based Intrusion Detection for Wireless Sensor Networks" Proceeding of IEEE International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing, pp. 272 - 279 , June 2008.
[25] Ilkar Onat, Ali Miri," An Intrusion Detection system for wireless sensor networks", Proceedings of IEEE International Conference on wireless and mobile computing networking and communication, pp.253-259,August 2005.

TABLE I: Advantages, Disadvantage and Future Scope of IDS

S.No.	Intruder Detection System	Advantage	Disadvantage	Future Scope
1.	Semantic IDS[7],[22]	Energy Efficient	Not Specific Decision Making Functions	Use more complex semantics for security
2.	Simple Learning Automata IDS[8],[24]	a. Energy efficient b. Optimized efficient packet sample.	Increased computational complexity	Can be used by more application which uses WSN
3.	Location Aware Trust based IDS[9]	a. Monitoring on the basis of Reputation	Not Energy efficient	Verification and Trusted Protocol can

		b. enhance integrity c. Efficiently detect Malicious node.		be used for future research
4.	Isolation table based IDS[10]	a. Accurate transmission b. More effective in case of live node.	Unreliable in case of less sensor nodes.	Isolation technique can be extended.
5.	Ranger based IDS[11]	Energy efficient in light weight model	Focuses only Sybil attack.	Can be used by many other protocol to evaluate performance
6.	Hierarchical overlay design based IDS[12]	a. Fast b. effective c. energy efficient d. reliable	Cost increased depends on policies.	Voting and election policy will be used.
7.	Hybrid IDS[13],[23]	a. More accurate b. high detection rate c. Increased network lifetime	Simulation is not used for performance evaluation	Rule based approach will be extended according to data mining.
8.	Weighted Trust Evaluation based IDS[14]	a. Little overhead in light weight model. b. easily nodes detection the basis of behaviour	High misdetection rate.	Performance evaluation research is going on
9.	Dynamic model of IDS[15]	More secure, stable and robust compare with static IDS	a. Time consuming b. not energy efficient	Can be applying on real application.
10.	Novel anomaly IDS[17],[25]	a. Low memory usage b. High detection accuracy c. low false alarm probability	a. Doesn't require a specification file for behaviour b. define only for small to middle size WSN	Can be extended for specification anomaly
11.	Embedded system based IDS (community IDS)[18]	a. lower power usage b. lower cost c. improved security defence ability of system. d. lower computer node	Depend only image processing arithmetic for analyzing the information	Sensing range can be extended using ranger IDS
12.	Immunity based IDS[19]	a. more robust, adaptive b. high accuracy in attack detection c. use co-stimulation for reducing no. of false positive.	Accurate high only with the immune algorithm.	Other beaconing protocol can be used
13.	Decentralized cluster and hash based IDS[20]	a. use rule based technique for interior intruder. b. use establishment phase knowledge for exterior intruder	Does not cover radio transmission and jamming rule	Will be verify the process of proposed solution experimentally
14.	Intelligent Transportation System based IDS[21]	a. simplify the routing problem b. solve the sensor localization problem	Depend on predefined path or flow of traffic	Will be implement on ns-2 simulation tool for performance evaluation