ISSN 2319 - 6629
Volume 3, No.3, April - May 2014
International Journal of Wireless Communications and Networking Technologies
Available Online at http://warse.org/pdfs/2014/ijwcnt01332014.pdf

A Survey on Intrusion Detection System in Wireless Sensor Networks

Manali Singh[1], Khushbu Babbar[2], Kusum Lata Jain[3]
Computer Science Department, Banasthali Vidyapith
C-scheme, Jaipur
[1]manali.singh.1989@gmail.com
[2]khushbu.babbar16@gmail.com
[3]kusum_2000@rediffmail.com

ABSTRACT

As wireless sensor networks continue to attract more attention, new ideas for applications are continually being developed, many of which involve consistent coverage of a given surveillance area. These networks are gaining importance in various applications like detecting temperature, pressure etc. but these systems are constrained by limited computational, memory and energy recourses. Security is one of the basic QoS requirements of wireless sensor networks, yet this problem has not been sufficiently explored. WSN are also vulnerable to various malicious attacks like sleep deprivation or battery drainage attack, cloning, jamming etc, when deployed in hostile terrain. So, security becomes an important factor when designing infrastructure and protocol of networks. Intrusion Detection is one of the methods of defending against these attacks. This paper presents a survey on various issues and security threats on WSN. This paper also discusses the recent trends in Intrusion Detection Systems along with implementation of IDS in WSN and comparative analysis of these schemes.

Keywords : Intrusion Detection System, Security Issues Types of IDS, Wireless Sensor Network (WSN)

1. INTRODUCTION

Wireless sensor network (WSN) is an emerging class of systems made possible by cheap hardware, advanced programming tools, complex and energy efficient radio interfaces. Wireless sensor network is a new paradigm in designing fault tolerant mission critical systems, to enable varied applications like threat detection, environmental monitoring, traditional sensing and actuation and much more. WSN is an emerging area of inter-disciplinary research between people in the electrical engineering, computer science, and among their various disciplines.
The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one or many sensors. Each sensor node of network has a radio transceiver, a microcontroller, a sensor and an energy source, usually a battery or an embedded form of energy harvesting. The main objective of sensor nodes is to collect information from its surrounding environment and transmit it to sink, called Base Station (BS). Sensor nodes are resource constraints. WSN are deployed in harsh and hostile terrain so are at high risk of physical distortion. Because of this intrinsic nature of networks, WSN becomes vulnerable to many security attacks. Many security mechanisms like authentication, key exchange and security routing have been proposed but they cannot deal with providing security towards many attacks. An IDS has provided with the best solution for addressing wide range of security attacks in WSN. This mechanism tries to identify systems and network intrusions and misuse by gathering and analyzing data. So, IDS monitor and analyze user and system activities against known attack patterns and identifies abnormal network activity and policy violations for WSN and then report to base station to avoid losing of any important data. This paper explores security issues in WSN in Section 2. Section 3 reviews attacks in WSN and section 4 discuss the type of Intrusion Detection Systems in WSN and their comparison. Finally Section 5 concludes the paper delineating the research challenges and future trends toward the research in wireless sensor network security.

2. SECURITY ISSUES IN WSN

A number of security issues are there with WSN and need to be analyzed in order to design appropriate security mechanisms and overcome security but designing new security protocols and mechanisms is constrained by the capabilities of the sensor nodes.

2.1 Hostile Environment

When sensor networks are deployed in remote or hostile environments such as battlefields physical attack becomes very easy as anyone can have access to their location. An attacker can easily capture a sensor node or even introduce his own malicious nodes inside the network thus compromising sensitive information. Also ill-disposed environment affects the monitoring infrastructure that includes sensor node and the network. Nodes failure and environment hazard causes topology changes and network partitioning thus making network topology more fragile.

2.2 Random topology

Due to random deployment in hostile environment, it is difficult to know the topology of sensor networks and it

becomes hard to store various encryption keys on nodes in order to establish encryption among a group of neighbors. Appropriate key distribution algorithms must be designed along a flexible WSN architecture to securely provide encryption keys in real time.

3. ATTACKS ON WSN

An attacker could organize attack in three phases: information gathering, exploits and contamination. So, attacker attempts to determine the characteristics and weaknesses of WSN by finding the location of the sink, traffic analysis, etc. Here we point out the major attacks in wireless sensor networks.

3.1 Jamming attack

In this attack, the attacker transmits the signal to the receiving antenna at the same frequency as the frequency used by the legal transmitter, which causes radio interferences. Jamming attack intends at disrupting communication services and results in partial or entire degradation of the services of the network. This attack can be made either by continuous emission of radio signal or transmitting only when channel is active rather than when channel is idle. Also injecting regular packets to channel without any gap between them or alternating between sleeping and jamming to save power consumption also causes jamming. This attack can easily be carried out by laptop with high energy.

3.2 Collision attack

In this attack, when attacker hears that a legitimate node is transmitting data, attacker sends its own signal for creating interferences. Even a collision of one byte can create error and cripple entire message. This is considered better than jamming attack in terms less power consumption and detection ability. This attacks aims at exhausting communication channel and degradation of network services.

3.3 Sinkhole attack

In this attack, the attacker node appears to be attractive to its neighboring nodes in terms of routing metric like higher power transmission or appearing as BS, because of which more and more of these neighboring nodes choose that attacker or sinkhole node to route their data. So this attack creates a false sink and exploits non authentication of links .and the result is that the information doesn't reach the BS thus damaging the network services.

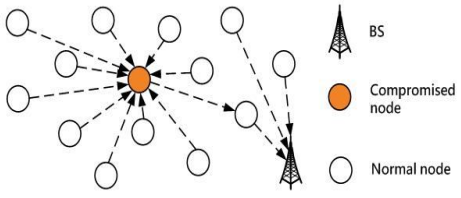
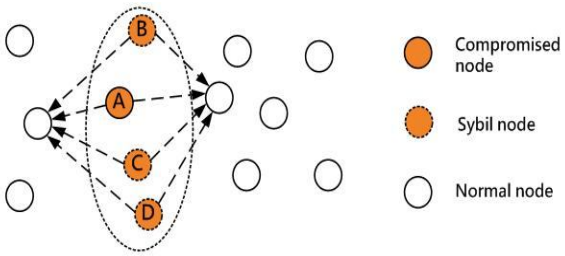


Figure 1: Sinkhole Attack in WSN

3.4 Sybil attack

In this attack, the attacker node assumes multiple identities and attempts to fill neighbor nodes memory with useless information that comes from these non existing neighbors attacker nodes fills others memory with redundant data and if the nodes have limit on number of nodes it keeps data of, it results in removal of actual nodes' information or even sink's identity. So, Sybil attack is an Identity attack, which causes unfairness in the network by forging as multiple nodes and thus creating information redundancy. It always aims at attacking data aggregation, voting etc services

Figure 2: Sybil Attack in WSN



3.5 Hello Flood attack

In this attack, the attacker node tries to convince all other nodes to choose it as parent node by using a powerful radio transmitter by flooding the entire network with hello message giving false neighbor status. Because of this false status, other legitimate nodes transmit data to this attacking node even though it might be out of range. This attack has same characteristics as Sybil attack but need more powerful radio.

3.6 Battery Drainage attack

In this attack, attacker forces the sensors to remain awake so that they waste their energy. Because of this large power is consumed by limited power sensor nodes. After exhausting, these sensors stop working and causes Denial of Services through Denial of Sleep.

3.7 Wormhole attack

In this attack, a low latency link or tunnel is created between two nodes in the network which then can be exploited by the attacker to attack on the nodes. This attack can aim at eavesdropping on data being transmitted, creation of false topology or authentication purpose. The result is same as that in Sinkhole attack. This attack requires a sophisticated radio or cable to establish the long channel communication.

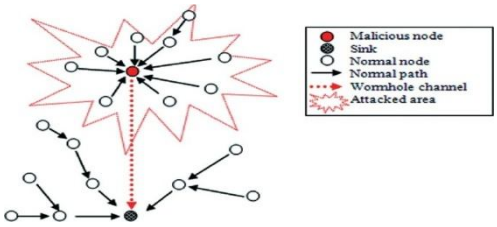


Figure 3: Wormhole Attack in WSN

4. INTRUSION DETECTION SYSTEM IN WSN

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS help in identifying and reporting unauthorized network activities and deny them access from network resources. IDS cannot be used as a stand-alone protection measure. Implementation of IDS faces many challenges in WSN. Some of them are: IDS require human intervention for proper implementation, technology used for IDS and it is reactive technology which finds the attacks on the basis of previous attack pattern.

5. CATEGORIES OF IDS

There are three major categories of IDS:

5.1 Signature-Based Intrusion Detection Systems

This IDS has some pre defined rules for security attacks. When packet traffic incomes, it is compared with these pre known signatures and if any activity is found to be deviated from these rules, its termed as an attack. Therefore this IDS is also called rule-based attack. But this IDS is only suitable for known intrusions and cannot detect attacks for which no rule has been defined. This IDS is basically used for detecting routing attacks and sinkhole attacks. Here every node monitors and cooperates with neighbors. Different signature-based IDS are given in Table 1.

Table 1: Signature-Based IDS

S.No.	Mechanisms	Attacks
1.	Collaborate	Black hole
2.	Local and cooperative detection	Sink Hole
3.	Genetic programming	Dos, unauthorized access
4.	Soft Computing	Unauthorized access, probing
5.	Specification based	Black hole, worm hole, repetition attack

5.2 Anomaly-based Intrusion Detection System

It is a heuristic approach is used to classify any network activity as malicious or normal. Generally some threshold values are used in which if an activity is below that threshold, its termed as normal or else as an intrusion. So this IDS uses statistical behavior modeling where audit data is taken for analysis by firstly transforming the data to format that is statically comparable to user's profile. This user's profile is dynamically generated by system administrator and updated on based of user's usage. Secondly thresholds are associated with all the profiles and if on analysis any deviation is found from threshold value, alarm of intrusion is raised. This IDS is capable of detecting new and unknown attacks. Different types of Anomaly-based IDS are given in Table 2.

Table 2: Anomaly-Based IDS

S.No.	Mechanisms	Attacks
1.	Artificial Neural Network	Time related changes
2.	Cluster based	Sink hole
3.	Support Vector	Black hole
4.	Cross Feature	Packet dropping
5.	Sliding window	Route depletion

5.3 Hybrid Intrusion Detection System

This IDS is a combination of signature based and anomaly-based IDS. This IDS consists of two detection modules, one for detecting well known attacks using rules or signatures and other module detects malicious patterns by detecting behavior deviation from normal patterns. This combination of two approaches makes hybrid IDS more accurate in terms of attack detection with less number of false positives. But this hybrid approach is usually not recommended in WSN as this consumes more energy and resources. In this technique sensor nodes are divided into cellular networks which are monitored by cluster heads and these cluster heads are monitored by regional nodes. Base station stores all the signatures and attacks are detected here. Different Hybrid IDS are given in Table 3.

Table 3: Hybrid IDS

S.No.	Mechanisms	Attacks
1.	State transition	Sync flood
2.	Cluster based	Routing attack
3.	Supervised learning	Routing attack
4.	Hierarchical and hybrid	Sink hole, worm hole

Table 4 shows comparison between various IDS approaches in terms of computation, energy and other designing issues.

Table 4: Comparison of Different IDS

Characteristics	Anomaly-based IDS	Signature-based IDS	Hybrid IDS
Detection rate	Medium	Medium	High
False alarm	Medium	Medium	Low
Computation	Low	Low	Medium
Energy consumption	Low	Low	Medium
Attack detection	Few	Few	More
Multilayer attack detection	No	No	No

Strength	Can detect new attacks	Detect attacks having signature	Detect both existing and new attacks
Weakness	Misses well known attack	Cannot detect new attacks	Require more computation and resources
Suitable for WSN	Yes	Yes	With justification

6. CONCLUSION

Most of the attacks against security in wireless sensor networks are caused by the insertion of false information by the compromised nodes within the network. A system is required for defending the inclusion of false reports by compromised nodes. IDS help in identifying and reporting unauthorized network activities and deny them access from network resources. Existing security schemes are based on specific network models However, developing a cost-effective and energy efficient false detection mechanism for all networks will incur a hard research challenge.

REFRENCES

1. OMKAR Pattnaik, Sasmita Pani. **Application of IDS in WSN: a survey** ,*IJRCCT*, Vol 1,issue 7, December 2012.
2. Nabil Ali Alrejah, S.Khan and Bibal Shams**. Intrusion Detection Systems in Wireless Sensor Networks: a review**, *International Journal of Distributed Sensor Networks*, Vol 2013.
3. Siebe Datema. **A case study of Wireless Sensor Network attacks**, Delft University of Technology, Sep 22th,2005.
4. Ruchi Bhatnagar, Dr, A.K. Srivastava, Anupriya Sharma. **An implementation Approach for Intrusion Detection System in Wireless Sensor Network**, *IJCSE*, Vol 2, no. 7,2010.
5. Rodrigo Roman, Jianying Zhou and Javier Lopez. **Applying Intrusion Detection System in Wireless Sensor Network.**
6. S. Khan, K. K. Loo, and Z. U. Din. **Framework for intrusion detection in IEEE 802.11 wireless mesh networks,** *International Arab Journal of Information Technology*, Vol. 7, no. 4, pp. 435–440, 2010.
7. Krontiris, t.Dimitriou and F.c. Freiling. **Towards intrusion detection in wireless sensor networks**, in proceedings of the *13th European Wireless Conference*, Paris, France, April 2007.
8. P.R. Da Silva, A.A.F. Loureiro, M.H.T. Martins, L.B. Ruiz, B.P.S. Rocha and H.C. Wong. **Decentralized intrusion detection in wireless sensor networks**, in proceedings of the *1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks (Q2winet '05)*, pp. 16-23, Montreal, Canada, October 2005.
9. M.S. Islam and S.A. Rahman,. **Anomaly intrusion detection system in wireless sensor networks: security threats and existing approaches**, *International Journal of Advanced Sciences and Technology*, Vol. 36, pp 1-8,2011.
10. Bhuse and A. gupta. **Anomaly intrusion detection in Wireless sensor networks**, *Journal of High Speed Networks*, Vol. 15, pp 33-51, 2006.
11. E. Loo, M.Y.Ng, C. Leckie and M. Palaniswami. **Intrusion Detection for routing attacks in sensor networks**, *International Journal of Distributed Sensor Networks*, Vol.2, no.4, pp 313-332, 2006.
12. I.Onat and Am Miri. **An intrusion detection system for wireless sensor networks**, *in Proceedings of IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob '2005)*, pp 253-259, August 2005.
13. R.Bhatnagar and U. Shankar. **The proposal of hybrid intrusion detection for defense of sync flood attack in wireless sensor network**, *International Journal of Computer Science and Engineering Survey*, Vol. 3, no. 2,pp 31-38,2012.
14. T.H.Hai, F.Khan and E.N.Huh. **Hybrid intrusion detection system for wireless sensor networks**, in *Computational Science and Its Applications-ICCSA* 2007,vol. 4706,pp 383-396.
15. K.Q.Yan, S.C.Wang,S.S.Wang and C.W.Liu**. A hybrid intrusion detection system of cluster-based wireless sensor networks,** in *Proceedings of the International MultiConference of Engineers and Computer Scientists(IMECS '09)*, Hong Kong, 2009.