INSERTION DETECTION TECHNIQUES USED IN WIRELESS SENSOR NETWORKS

Vijay Pal Singh[1], Dr. Ruchira Bhargava[2] and Dr. Satyaveer Singh[3]

[1]Research Scholar, Department of CSE, Shri JagdishPrasad Jhabarmal Tibrewala University, Jhunjhunu (Rajasthan)
Email: tilotiya09@gmail.com
[2]Associate Professor (HOD), Department of CSE, Shri JagdishPrasad Jhabarmal Tibrewala University, Jhunjhunu (Rajasthan)
Email: dr_ruchira@yahoo.in
[3]Associate Professor (HOD), Departmentt of Mathematics, Shri JagdishPrasad Jhabarmal Tibrewala University, Jhunjhunu (Rajasthan)
Email: drsbhaira@gmail.com

ABSTRACT

Wireless Sensor Networks (WSN) is one of the hottest areas over the past few years. The number of the potential applications, involving WSNs dictates that they should be secure. In this paper we will show the major threats that WSNs have to deal with. Additionally we will mention existing countermeasures, further we will focus on intrusion detection. We combine existing IDS approaches and show the steps to build an IDS for WSNs. we discuss the general guidelines for applying IDS to static sensor networks, and introduce a novel technique to optimally watch over the communications of the sensors' neighborhood on certain scenarios.

Keywords: Wireless Sensor Networks, Internet Security, IDS.

Intrusion Detection Issues in WSN

Even though there are many proposed IDSs for wired networks, WSN specific features make conventional IDSs ineffective and inefficient for this new environment. Consequently, researchers have been working recently on developing new IDSs for WSN or changing the current IDSs to be applicable to WSN. There are new issues which should be taken into account when a new IDS is being designed for WSN.

There are four aspects of a wireless sensor network that security must protect:

- Confidentiality
- Data Integrity
- Service Availability
- Energy

The first three are addressed by security systems in wired networks and non-energy-constrained wireless networks, but the fourth one is unique to the sensor network application.

Lack of Central Points in WSN does not have any entry points such as routers, gateways, etc. These are typically present in wired networks and can be used to monitor all network tracks that pass through them. A node of a WSN can see only a portion of a network: the packets it sends or receives together with other packets within its radio range.

Wireless Links Wireless networks have more constrained bandwidth than wired networks and link breakages are common. IDS agents need to communicate with other IDS agents to obtain data or alerts and need to be aware of wireless links. Because heavy IDS track could cause congestion and so limit normal track, IDS agents need to minimize their data transfers Bandwidth limitations may cause in active IDS operation. For example, an IDS may not be able to respond to an attack in real-time due to communication delay. Furthermore, IDS agents may become disconnected due to link breakages. IDS must be capable of tolerating lost messages whilst maintaining reasonable detection accuracy.

Proposed Intrusion Detection Systems in WSN

In this paper the proposed IDS's on WSN are reviewed to find out how well they address the IDS issues explained above. The following criteria are used in this survey:

Input Data Intrusion detection systems can use host audit data, network packets or statistics of such data (e.g. statistics of updates in routing tables and the number of received packets in the last 10 seconds).

Detection Method The most commonly proposed intrusion detection method in WSN to date is specification-based detection. This can detect attacks against routing protocols with a low rate of false positives. However, it cannot detect some kind of attacks, such as DoS attacks. There are also some anomaly-based detection systems implemented in WSN. Unfortunately, mobility of WSN increases the rate of false positives in these systems. There have been few signature-based IDS's developed for WSN and little research on signatures of attacks against WSN. Updating attack signatures is an important problem for this approach.

Decision-Making Two different decision-making mechanisms are used in distributed and cooperative IDS's: collaborative decision-making, where each node can take active part in the intrusion detection process, and independent decision-making, where particular nodes are responsible for decision-making. Both decision-making mechanisms have pros and cons. Collaborative-decision making systems are more reliable. If all nodes contribute to a decision, a few malicious nodes cannot easily disrupt the decision-making. However, if any node can trigger a full-force response, it can react the entire network and be vulnerable to a DoS attack. A collaborative-decision making approach is also more resilient to benign failure of nodes. On the other hand, failing or compromise of particular nodes in independent decision-making systems can have drastic acts. However, these systems are less prone to spoofed intrusion attacks than collaborative decision-making systems.

Response Mechanism The system can have a passive response or an active response to detected intrusions. Reputation systems reviewed in are example methods used on WSN for active responses.

IDS testing this are the area of IDS testing and evaluating its effectiveness and efficiency. IDS Security There can be attacks against IDS itself; this feature is the degree of IDS security in opposition to these attacks.

Feature	Explanation	Classification
Input Data	Monitored data	Network packets, MIB data, host data, statistic, etc.
Data Gathering	From where data is gathered	Host-participatory or promiscuous Listening
Architecture	Structure and organization of IDS agents	Standalone, distributed and cooperative, hierarchical
Grouping	How to group distributed IDS Agents	Clusters, zones, one-hop away nodes
Interoperability	How to communicate with IDS agents	Network packets or mobile agents
Detection Method	Method used to detect Intrusions	Anomaly-based, specification-based, misuse-based
Decision Making	How to make decisions about Intrusions	Local, collaborative or independent
Response Mechanism	How to react to detected intrusions	Passive or active response (on controlled or on controlling system)
IDS Security	Vulnerabilities of IDS agents	Single point of failure, attacks against mobile agents, DoS attacks, etc.

All these features above are summarized in Table: Survey Features

Intrusion Detection Using Multiple Sensors

IDS solution based on mobile agent technology which reduces network load by moving computation to data. This is a significant feature for WSN which have lower bandwidth than wired networks. A modular IDS structure is proposed that distributes the functional tasks by using three mobile agent classes: monitoring, decision-making and action-taking. The advantages of this structure are given as increased fault-tolerance, communication cost reduction, improved performance of the entire network, and scalability.

A hierarchical and distributed IDS architecture is given which divides the network into clusters. Cluster heads are chosen by vote, with each node voting for a node based on its connectivity. Each node in the network is responsible for local detection using system and user level data. Only cluster heads are responsible for detection using network level data and for making decisions. However, depending on the hop attribute of the clusters, network intrusion detection performance can change. For example, every node has direct connection to at least one cluster head in a one-hop clustered network (nodes 1, 2, 5, and 8 are cluster heads), so each packet in the network can be monitored as shown in Figure (a), while three links in Figure (b) cannot be monitored by the cluster-heads in a two-hop clustered network (nodes 1, 2, and 5 are cluster-heads). As the degree of monitoring increases the number of cluster heads increases too. So, choosing the hop attribute of the clusters is a trade-off

between security and efficiency. However, the nodes not in a cluster heads communication range can move to the monitoring area of another cluster head due to mobility. Having a few links that cannot be monitored by any cluster head is regarded as acceptable for highly dynamic environments.

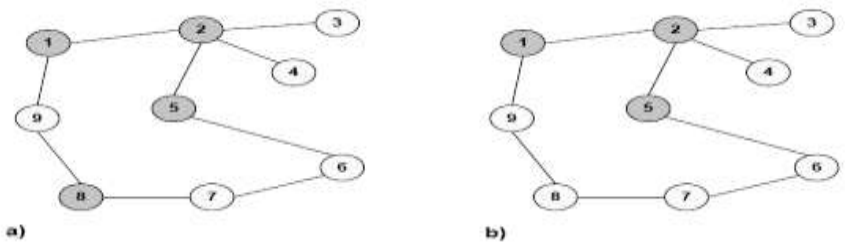

Figure:1 IDS Architecture

(a) One-hop Clustered Network (b) Two-hop Clustered Network Cluster nodes can respond to the intrusions directly if they have strong evidence locally. If the evidence is insufficient they leave decision-making to cluster heads by sending anomaly reports to them.

In this paper a scalable and bandwidth-efficient IDS is proposed by using mobile agents but without giving any validation via simulation or implementation. On the other hand, there are urgent security issues for mobile agents that are set to be investigated in their future research. In addition, details of the anomaly-based detection method are not given, with research on more robust and intelligent cooperative detection algorithms left as future research.

Future Research

WSN are a new type of distributed network whose properties are complex and ill-understood. Intrusion detection on these complex systems is still an immature research area. There are far fewer proposed IDSs for WSN than for conventional networks. Researchers can focus on either introducing new IDSs to handle WSN specific features or can adapt existing systems. Hybrid approaches may also prove of significant use.

As stated earlier, intrusion detection in WSN poses special problems. Table shows each proposed IDS reviewed in this chapter, identifying any novel contributions together with an indication of notable issues they do not address. They usually emphasize just a few specific WSN concerns. The range of WSN issues should be considered during design to ensure effective and efficient intrusion detection suited to the environment at hand.

We make the following observations about the proposed IDSs:

- The systems generally cover restricted sets of attacks.
- The systems usually target a specific protocol.
- Some proposed IDS systems do not take into account mobility of the network.
- Inadequate acknowledgement is given to the resource constraints that many nodes are likely to be subject to, and to the likelihood of nodes with different capabilities.

- Several network architectures proposed do not t well with the dynamic nature of WSN.
- A more extensive evaluation of many of the systems would seem appropriate.

The proposed systems seek to address the lack of central points issue on WSN by proposing distributed and cooperative IDS architectures. Such architectures raise questions about security, communication and management aspects. Suitability of the architecture to the environment is an important consideration in designing IDS. Architecture should not introduce new weaknesses/overheads to IDS. For instance, some of the proposed architectures like cluster-based approaches are costly to build and maintain for high mobility networks. Some have critical points of failure.

CONCLUSION

WSN are a new technology, increasingly used in many applications. These networks are more vulnerable to attacks than wired networks. Since they have different characteristics, conventional security techniques are not directly applicable to them. Researchers currently focus on developing new prevention, detection and response mechanism for WSN.

We have given a survey of research on IDS for WSN. Many WSN IDSs have been proposed, with different intrusion detection techniques, architectures, and response mechanisms. We have focused on the contribution/novelty each brings and have identified the specific WSN issues each does not address. Proposed systems generally emphasis on few WSN issues, it have most of the problems of wired networks and many more besides. As a consequence intrusion detection for WSN remains a complex and challenging topic for security researchers.

REFERENCES

1. Abraham and C. Grosan. Evolving intrusion detection systems. In Genetic Systems Programming: Theory and Experiences, volume 13, pages 5779. Springer, 2006. 89, 91
2. A.Abraham, C. Grosan, and C. Martiv-Vide. Evolutionary design of intrusion detection programs. International Journal of Network Security, 4:328339, 2007. 89
3. B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens. An on demand se-cure routing protocol resilient to byzantine failures. In Proceedings of the ACM Workshop on Wireless Security, 2002. 37
4. J. Kong, X. Hong, and M. Gerla. A new set of passive routing attacks in mobile ad hoc networks. In Proceedings of the IEEE Military Communications Conference (MILCOM), 2003. 33
5. P. Kazienko and P. Dorosz. Intrusion detection systems (IDS), 2004. http://www.windowsecurity.com/articles/IDS-Part2-Classification-methods-techniques.html
6. Y. Li and J. Wei. Guidelines on selecting intrusion detection methods in WSN. In Proceedings of the Information Systems Educators Conference, 2004.21, 29
7. B. Sun, K. Wu, and U.W. Pooch. Zone-based intrusion detection for mobile ad hoc networks. International Journal of Ad Hoc and Sensor Wireless Networks, 2(3), 2003. 7,

32, 51, 52, 53, 75, 81

8. O. Kachirski and R. Guha. Effective intrusion detection usign multiple sensors in wireless ad hoc networks. In Proceedings of the 36th IEEE International Conference on System Sciences, 2003. 7, 46, 47, 49, 54, 55, 117
9. S. Axelsson. Intrusion detection systems: A survey and taxonomy. Technical Re-port 9915, Department of Computer Engineering, Chalmers University of Technology, 2000. 41, 43
10. R. Heady, G. Luger, A. Maccabe, and M. Servilla. The architecture of a network level intrusion detection system. Technical report, Computer Science Department, New Mexico
11. T. Anantvalee and J. Wu. A survey on intrusion detection in mobile ad hoc networks. In Wireless Network Security, pages 159180. Springer, 2007.45, 46, 73
12. X. Wang, T. Lin, and J. Wong. Feature selection in intrusion detection system over mobile ad-hoc network. Technical report, Department of Computer Science, Iowa State University, 2005. 73, 75