National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing (RTMC) 2011
Proceedings published in International Journal of Computer Applications® (IJCA)

Alternate Path Approach to Avoid Intrusion Detection in Wireless Sensor Networks

Ajay Gautam[1]Ritu[2]Naveen Sharma[3]

Department of CSE, MMEC, Mullana, MM University Mullana, India[1, 2]
Department of CSE, SITM, Rewari, MD University Rohtak, India [3]

ABSTRACT

Wireless Sensor Network (WSN) is a new computing paradigm that emerged from the fusion of the SCADA systems and Ad hoc networks technologies. WSN derives the networking characteristics of ad-hoc network and combines it with the hardware facilities of tiny wireless sensors. Once a sufficient number of nodes have been deployed, the sensor network can be used to fulfill its task, such as measuring the physical variables. This task can be issued and supervised by an external entity connected to the WSN, such as manager or supervisor. Due to insecure nature of the wireless link and the dynamically changing topology, wireless ad-hoc networks require a careful and security oriented approach for designing protocols. Also any node can join or leave the network at any time. This is security breach as the joining node can be a malicious node and can have unwilling effects on the network performance. So it is very important to authenticate the joining nodes from the establishment of the network. Cluster based architecture is used because it is easily manageable and more secure than other architectures. In cluster based architectures gateways are used for inter cluster communication. The aim of this article to proposes the new cluster base security architecture which starts from the initialization of the network.

1. INTRODUCTION

WSNs are increasingly attractive tools to detect, monitor and control environmental conditions. WSNs can be used to bridge the gap between the physical and the virtual world. WSNs have a variety of applications of distributed wireless sensing including medical, home security, machine diagnosis, military applications, environmental monitoring, chemical/biological detection, precision agriculture, etc. Micro sensors of WSN must be designed in a highly integrated way with the goal of optimizing energy dissipation, limited computation and self-configuration. WSNs must be self-directed and require a high degree of cooperation and adaptation to perform the desired coordinated tasks, so that the WSN as a whole can provide functionality that an individual node can’t. Micro sensors will be able to coordinate among themselves on a higher-level sensing task (e.g., reporting the speed, direction, size, and other characteristics of a moving vehicle). Figure shows the concept of WSN.

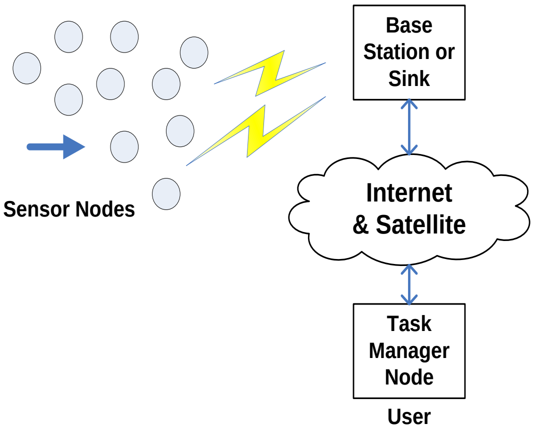


Fig. 1: Wireless Sensor Network (WSN)

Within few years, sensor integration and electronic miniaturization will make possible to produce extremely cheap sensing devices. These devices will be able to monitor and control wide variety of ambient conditions: temperature, pressure, relative humidity, viscosity, soil makeup, vehicular movement, noise levels, moisture, lighting conditions, mechanical stress levels, and so on. Smart sensor alone can be used to measure the many physical parameters such as temperature, pressure, speed, etc.

1.1. Sensor Network Challenges

Support for very large numbers of unattended autonomous nodes, adaptability to environment and task dynamics in are the fundamental challenges of WSNs as they have limitations of dynamic network topology, limited battery power, and constrained wireless bandwidth. The configuration of sensor nodes would frequently change in terms of position; reach ability, power availability, and even task details. Because these sensor nodes interact with the physical environment, they would experience a significant range of task dynamics. Node mobility, node failures, and environmental obstructions cause a high degree of dynamics in WSN. This includes frequent network topology changes and network partitions. The partitioned sub networks need to continue running independently and the management protocol must be robust enough to adapt this condition. Sensors are energy constrained and subject to unfriendly environments; they can store or reproduce very limited energy from the environment. That is why they fail due to depleted batteries or due to environmental influences. Restricted size and energy typically means restricted resources (CPU performance, memory, wireless communication bandwidth and range). Thus, we need to ensure that network protocol overhead is kept to a minimum so that energy is conserved. The number of packets transmitted/received/processed at each node should be reduced since energy is consumed in these operations. WSN middleware should support the implementation and basic operation of WSN as outlined above. However, this is a not a trivial task, as WSNs have some unique properties different from ad hoc networks. To outline this point, the differences between sensor networks and ad hoc networks are illustrated below:

1) Sensor nodes are densely deployed in compare to the ad hoc network nodes.

2) The WSN has larger number of sensor nodes than a hoc network.

3) WSN network topology changes more frequently than ad hoc network.

4) WSN nodes are inclined to fail more than ad hoc network nodes.

5) WSN nodes are scarce in resources such as limited in power, and memory.

1.2. Wsn Applications

The features described above provide a wide range of applications for WSNs. WSNs may consist of numerous diverse kinds of sensor nodes to sense different types of parameters such as acoustic, thermal, visual, magnetic, infrared, seismic, radar, etc. These sensor nodes are able to monitor a wide variety of ambient conditions that include the following: flow, temperature, pressure, humidity, moisture, noise levels, mechanical stress, speed, etc. Smart sensors that can monitor many physical variables can be used with WSN. Many new applications are being developed because of this new concept of micro sensing and wireless networking of these smart sensors. Some of the potential diverse applications of WSNs are as follows: temperature control, inventory management, physiological monitoring, habitat monitoring, precision agriculture, forest fire detection, nuclear, chemical, and biological attack detection, military, transportation, disaster relief, and environmental monitoring (air, water, and soil chemistry). WSNs can reform information gathering in a variety of situations.

1.3. SECURITYCONSIDERATIONS

Intrusion detection

An Intrusion detection system (IDS) is software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling of computer mainly through a network, such as the Internet. These attempts may take the form of attacks, as examples, by crackers,, malware and/or disgruntled employees. IDS cannot directly detect attacks within properly encrypted traffic. An intrusion detection system is used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and viruses.IDS can be composed of several components: Sensors which generate security events, a Console to monitor events and alerts and control the sensors, and a central Engine that records events logged by the sensors in a database and uses a system of rules to generate alerts from security events received. There are several ways to categorize IDS depending on the type and location of the sensors and the methodology used by the engine to generate alerts. In many simple IDS implementations all three components are combined in a single device or appliance.

Intrusion Prevention

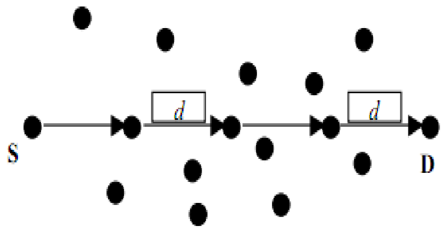
Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators. In addition, organizations use IDPSs for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies. IDPSs have become a necessary addition to the security infrastructure of nearly every organization.

2. PROBLEM DEFINITION

Intrusion is one of the common problems in all network, in case sensor network we face the same problem. When we have a denser sensor network with no of nodes and there is some important data is transferring over the network, there is the requirement of security. But in case of “man in middle” it is never easy to say a network is intruder safe. Even when the Intruder knows about the routing algorithms or the algorithm implementation it is quite difficult to handle the problem.

One of such algorithm is generally followed by a user over the network is the shortest path problem, When intruder want to hack some information by acting man in middle, it is not easy for him to trace all the nodes over the network because the sensor network contains large number of nodes.

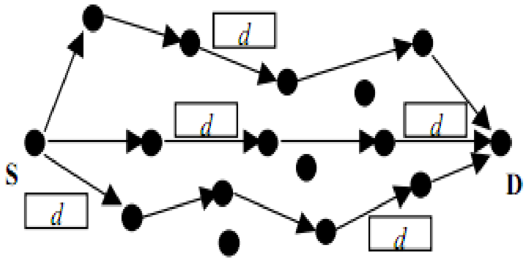
In such case instead of tracking each node, intruder follows a route or the pattern to perform the attack. One of such method is to trace the shortest path. Generally each routing algorithm follows the concept of shortest path to transfer the data over the network with minimum time requirement. In other words we can say shortest path route nodes are the most unsafe nodes for transferring data as they are generally targeted by the intruder.



Next after the whole mechanism is being defined the mechanism must be analyzed for the security breaches and any security breach must be removed form it. The mechanism has the possibility of an attack i.e. man in middle attack. The attack can be performed by the intermediate node i.e. malicious node and have the unwilling effects on the ongoing process. The solution to the attack is given by finding an alternative route to the destination node and by getting the proper acknowledge from the destination node.

3. PROPOSED SYSTEM

Due to insecure nature of the wireless link and the dynamically changing topology, wireless ad-hoc networks require a careful and security oriented approach for designing protocols. Also any node can join or leave the network at any time. This is security breach as the joining node can be a malicious node and can have unwilling effects on the network performance. So it is very important to authenticate the joining nodes from the establishment of the network. Cluster based architecture is used because it is easily manageable and more secure than other architectures. In cluster based architectures gateways are used for inter cluster communication. The thesis proposes the new cluster base security architecture which starts from the initialization of the network. The network establishment takes place from the starting i.e. there is initially no nodes in the network. The authentication of the joining new nodes is done by using hash functions. As the network grows the architecture enables the network to be divided into number of clusters and each cluster having a cluster head. The cluster head has the responsibility for managing the whole cluster. After the different nodes being divided into number of cluster, there is secure communication mechanism for inter and intra cluster communication. Finally the thesis addresses the attack possibility on the scheme.



The attack possible is man in middle attack. The possible solution is given to the attack which uses the alternative route finding algorithm. The technique uses the method to find the alternative route which is not the shortest and which doesn’t involve any node that resides in the shortest path. We simulate the proposed solution using our own simulator developed in C#

4. CONCLUSION

Importance of WSN cannot be denied as the world of computing is getting portable and compact. Unlike wired networks, WSN pose a number of challenges to security solutions due to their unpredictable topology, wireless shared medium, heterogeneous resources and stringent resource constraints etc. The Security research area is still open as many of the provided solutions are designed keeping a limited size scenario and limited kind of attacks and vulnerabilities. We are providing the solution for the problems where we can save the ad hoc network from the active attack of Intruders that are on the basis of algorithmic implementations. Generally the path selected for data transfer in ad hoc network is the shortest path because of this intruder attack is also in same area. We have generated such a path in which no node from the shortest path will be included. It will give an secure and efficient approach of data transmission in ad hoc network in unit cast.

5. REFERENCES

[1] E. Guillen, D. Padilla, and Y. Colorado, “based Intrusion Detection and Prevention Systems,” Latin-American Conference Communications, 2009, pp.

[2] T. Ghorbani, A.A., Lu, W., Network Intrusion Detection and Prevention: Concepts and Technique, Springer, 2009...

[3] T. Dutkevych, A. Piskozub, and N. Tymoshyk, “Real-Time Intrusion Prevention and Anomaly Analyze System for Corporate Networks,” IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems Technology and Application, 2007, pp. 599-602.

[4] E.E. Schultz and E. Ray, “Future of Intrusion Prevention,” Computer Fraud & Security, 2007, pp. 11-13.

[5] H.S. Rhee, C. Kim, and Y.U. Ryu, “Self-efficacy in information security: Its influence on end users’ information security practice behavior,” Journal Computer & Security, vol. 28, 2009, pp. 816-826.

[6] V. Frias-martinez, J. Sherrick, S.J. Stolfo, and A.D. Keromytis, “A Network Access Control Mechanism Based on Behavior Profiles,” Annual Computer Security Applications Conference, 2009, pp. 3-12.

[7] W. Kim, O.K. Jeong, and S.W. Lee, “On social Web sites,” Journal of Information Systems, vol. 35, 2010, pp. 215-236.

[8] C.Y. Wang, S.-cho T. Chou, and H.-ching Chang, “Emotion and Motivation: Understanding User Behavior of Web 2. 0 Applications,” IEEE Computer Society Seventh Annual Commnucation Networks and Services Research Conference, 2009, pp. 1341-1346.

[9] S.X. Wu and W. Banzhaf, “The use of computational intelligence in intrusion detection systems: A review,” Applied Soft Computing, vol. 10, 2010, pp. 1-35.

[10] A.D. Todd, R.A. Raines, R.O. Baldwin, B.E. Mullins, and S.K. Rogers, “Alert Verification Evasion Through Server Response Forging,” Alert Verification Evaluation Through Server Response Forging, LNCS, vol. 4637/2007, 2007, pp. 256-275.