ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)

On 21st & 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

Trust Management Based Intrusion Detection in Wireless Sensor Networks

Mr.R.Mohan Kumar[1] Dr.A.V.Ramprasad [2]

[1]Departmentof ECE, K.L.N College of Engineering, Madurai, India

[2]Departmentof ECE, K.L.N College of Engineering, Madurai, India

ABSTRACT— In wireless sensor network (WSN), intrusion acts as a serious threat impairing the network, it is necessary to refrain from these attacks by the detection of intrusion which turns out to be a challenging task. Apart from these hazards there prevail other kinds of deterrent attacks. The overall intrusion can be curbed down by80%. In this work , consider trust based nodes in a route for transmission of information from the source to destination. The centralized and decentralized wireless sensor networks are taken into account through which the trust behaviors of nodes are determined. In decentralized wireless sensor network, the leader or cluster head is designated based on the energy levels of the nodes. Region wise election is established for the selection of the cluster head or leader depending on the factors of runtime, area and energy. A trust management protocol is deployed which facilitates the analysis of trust behavior of nodes in a route .In our approach , use a centralized wireless sensor networks, such that a single leader is responsible for collecting all information of sub leaders and if intrusion evolves in the network, it overcome by transmitting the data through these trustable nodes. The intruders in the route are found by using a intrusion detection system protocol (IDSP) thereby by eliminating degradation of transmission**.**

KEYWORDS: WSN, De-Centralized, IDSP, Cluster

I.INTRODUCTION

A WIRELESS sensor network (WSN) is usually composed of a large number of spatially distributed autonomous sensor nodes (SNs) to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants. A SN deployed in the WSN has the capability to read the sensed information and transmit or forward information to base stations or a sink node through multi-hop routing.

A more serious issue is that nodes may be compromised and perform malicious attacks such as packet dropping or packet modifications to disrupt normal operations of a WSN where in SNs usually perform unattended operations. A large number of SNs deployed in the WSN also require a scalable algorithm for highly reconfigurable communication operations; propose a hierarchical trust management Protocol leveraging clustering to cope with a large number of heterogeneous SNs for scalability and re-configurability, as well as to cope with selfish or malicious SNs for survivability and intrusion tolerance.

II. TRUST ANALYSIS

A. TRUST:

TRUST in general is the level of confidence in a person or a thing. Various engineering models such as security, usability, reliability, availability, safety, and privacy models incorporate some limited aspects of trust with different meanings. For example, in sensor network security, trust is a level of assurance about a key's authenticity that would be provided by some centralized trusted body to the sensor node (SN). In wireless ad hoc and sensor network reliability, trust is used as a measure of node's competence in providing required service. In general, establishing trust in a network gives many benefits such as the following:

1. Trust solves the problem of providing corresponding access control based on judging the quality of SNs and their services. This problem cannot be solved through traditional security mechanisms.

2. Trust solves the problem of providing reliable routing paths that do not contain any malicious, selfish, or faulty node(s).
3. Trust makes the traditional security services more robust and reliable by ensuring that all the communicating nodes are trusted during authentication, authorization, or key management.

For Wireless Sensor Networks (WSNs), visualize that trust management is a cooperative business rather than an individual task due to the use of clustering schemes such as LEACH, PEGASIS, TEEN, and HEED in real-world scenarios. Moreover, SNs can also be deployed in the form of groups, which are willing to collaborate with each other in order to process, aggregate, and forward collected data. This highlights the fact that these clustering schemes and group deployments enable SNs to fulfill their responsibilities in a cooperative manner rather than individually. Therefore, establishing and managing trust in a cooperative manner in clustering environment provides many advantages. Such as, within the cluster, it helps in the selection of trusted cluster head by the member nodes. Similarly, the cluster head will be able to detect faulty or malicious node(s).

In case of multi hop clustering, it helps to select trusted en route nodes through which a node can send data to the cluster head. During inter cluster communication, trust management helps to select trusted en route gateway nodes or other trusted cluster heads through which the sender node will forward data to the base station (BS).

B. Mobile Ad-Hoc Network

A mobile ad hoc network (MANET) is a dynamic wireless network with or without fixed infrastructure. Nodes may move freely and organize themselves arbitrarily. Sparse MANETs are a class of ad hoc networks in which the node population is sparse, and the contacts between the nodes in the network are infrequent. As a result, the network graph is rarely, if ever, connected and message delivery must be delay tolerant. Traditional MANET routing protocols such as AODV, DSR, DSDV, and LAR make the assumption that the network graph is fully connected and fail to route messages if there is not a complete route from source to destination at the time of sending. These schemes are sometimes referred to as mobility-assisted routing that employ the store-carry-and-forward model. Mobility-assisted routing consists of each node independently making forwarding decisions that take place when two nodes meet. A message gets forwarded to encountered nodes until it reaches its destination.

III. INTRUSION DETECTION SYSTEM ANALYSIS

An IDS – INTRUSION DETECTION SYSTEM is one of many tools that an organization may use to help determine if their network or server environment has experienced an unauthorized intrusion. An IDS may be used as hardware installed on the network or as an agent on an existing piece of hardware that is connected to a network. The IDS has often been compared to a house alarm system, which it does act like in the sense of providing an alert when a predefined event occurs. Unlike a house alarm, it will provide the type of event that occurred, when and where in the network/server environment the intrusion occurred and the source of the intrusion.

IV. SINK-HOLE ATTACK DESCRIPTION

A sinkhole attack in wireless sensor networks can cause serious problem in the operations and services of the networks. It may lead to the problem of system failure in terms of network availability (6). And it makes the sensor node unable to transmit and receive information. It is a kind of denial of service attack where a malicious node can attract all packets by falsely claiming a fresh route to the destination and without forwarding them to the destination. Because in Tiny AODV (7), there is no single destination for messages, such as a base station, a sinkhole cannot imitate a node and attract traffic towards it. To get as much influence on routes as possible, a sinkhole will have to take action every time a route is being created.

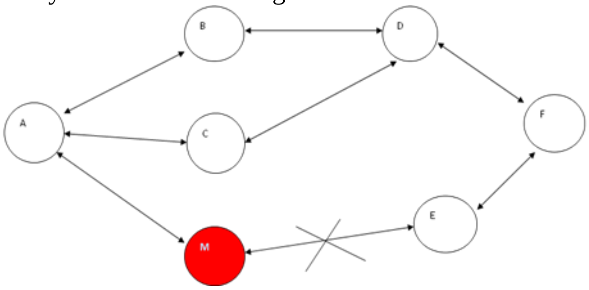

Fig 1: Intruder inside the Route from source to Destination

There is a node in the route, where it will collect all the information from the source and it won't send it to the next node. It intrudes the data which ever comes from the source node.

V. LEADER BASED ELECTION

In this approach LBIDS, a leader is elected for solving the IDS in the WSN, it is a cost effective and resource effective approach. In this technique the WSN area is splitted into regions. Each region is considered as a sub-network. All the M number of regions might have N number of nodes, and each node is assigned with initial energy value of 100. There is a cluster C, which should be in centre to other nodes and it has the highest energy value than all the nodes. In the initial stage, a random node is considered to be a leader node and the other nodes are regular nodes.

At the time of data transaction the leader will be elected dynamically due to the energy level, which is having the highest energy in the network region. Hence all the regular node enables communication region to region through the cluster nodes of their region. While transaction of data from one node to the other in the cluster evaluates the information from all the nodes in the route from source to destination. Example A->B->C->E->F, means from A to F, B,C,E are the intermediate nodes. If and only if the cluster knows about all the nodes, it permits the source to send the data to the destination, otherwise, it indicates the occurrence of malicious node in the route.

VI. **INTRUSION DETECTION IN WSN**

Propose an Intrusion Detection System (IDS) node selection method for Wireless Sensor Networks (WSNs). Due to the WSNs' distinctive tree structure, network congestion normally occurs in nodes that are located in the vicinity of a static base station. Moreover, in resource-constrained WSNs, network congestion could occur due to resource depletion attacks, such as Denial of Service (DoS) attacks. This congestion increases data loss and reduces the network's lifetime. In this work, propose an Intrusion Detection Systems (IDSs) construction method that considers this network congestion. Moreover, due to the limited battery life of sensor nodes, the proposed method is considered to be efficient in utilizing limited resources by selecting IDS nodes that enhance the network's lifetime and reduce the total energy consumption. The simulation results show that the proposed method enhances the network's lifetime and reduces the total energy consumption of the congested network.

An Intrusion Detection System (IDS) for wired networks is widely employed for security purposes to detect illegal intrusions that are considered to be unauthorized or abnormal [2]. However, most intrusion detection techniques are not suitable for wireless networks since they utilize open media and collaborative algorithms and lack centralized monitoring and management points [3, 4]. Therefore, an ad hoc intrusion detection architecture is needed for wireless networks. Especially in WSNs, besides the problems mentioned above, the IDS has to solve the problems imposed by the limited battery life and computational power of sensors.

To secure mobile computing applications, an anomaly intrusion detection architecture (AD) is proposed, in which every node in the wireless network participates in intrusion detection [3]. The AD scheme provides intrusion detection facilities into wireless nodes, and they are called IDS nodes. As an IDS node overhears and analyzes all packets within its monitoring range, the IDS node consumes more resources than non-IDS nodes [2]. In terms of limited network resources, the AD scheme, which has many IDS nodes in the network, is inefficient. Moreover, the major problem with this approach is that one node usually receives the same monitoring services from all neighbor IDS nodes. Therefore, an efficient IDS node selection method is needed in order to utilizing the limited wireless network resources. For selecting IDS nodes in wireless networks, a distributed IDS node selection scheme (DIDS) is proposed for wireless ad hoc networks that allocates intrusion detection tasks to nodes with high connectivity.

VII**. ANALYSIS OF DATA TRANSMISSION**

This shows how sinkhole is happening. There are number of nodes in a wireless sensor network, where the node 0 is consider as source node and the node 6 is considered as destination node. While transferring the data from source to destination, the source node sends the request and receives response from other nodes and finds the route. In this scenario, initially the node 3 sends response to the source node and stores the received data from the source node. The source node now awaits for an acknowledgement from the destination node. If no such acknowledgement is received, the source node then suspects the node 3 to be the sinkhole node and displays it.

After suspecting the sinkhole node, the source node applies [Routing Algorithm], i.e., in each stage all the source nodes receives the next neighboring node by applying the formula

$$TAB = (R-d)/V \ (R>d) \quad -----(1)$$

Where R is the transmission range; d is the distance between the node A and node B; V is the average speed of the node. This indicates∀ Nodes A and B, node A and node B are neighbors if they are within each other's transmission range R and are called the neighboring nodes. Also for Nodes A and B, node A and node B are neighbours if they are within each other's transmission range R and are called the neighboring nodes. Also for Nodes A and B, node A and node B are neighboring nodes, if the distance between them is TAB. To overcome this sinkhole attack it chooses the other node to send the data packets because in wireless sensor network most of the nodes are alive nodes or beacon nodes. In the remedy for sinkhole attack when the path size will be increases the packet loss will be occur and also are not able to monitor the intruder clearly in each region when the node will get change. So , go for newly derived approach known as LBIDS.

A.Centralized And De-Centralized Network:

In decentralized sensor network, the leader or cluster head is elected based on the energy levels of the nodes. This cluster head or leader is also chosen region wise based on runtime, area and energy. The data wireless or packet transmission takes place through the trustable nodes along the route. Use a trust management protocol for trust behavior analysis of nodes. In this work , use a centralized wireless sensor networks, where a single leader is responsible for collecting all information of sub leaders which in turn is elected based on the trust behavior of the nodes. If intrusion occurs it is detected by intrusion detection protocol (IDSP) and the data transaction takes place through the trustable nodes in the route.

B.Simulation Analysis:

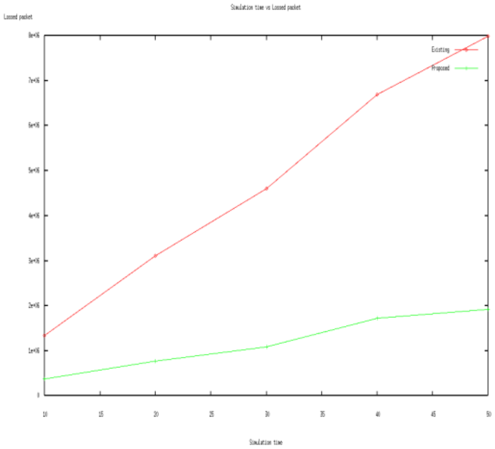

Fig 2: Comparison Between Simulation Time Vs Lossed Packets

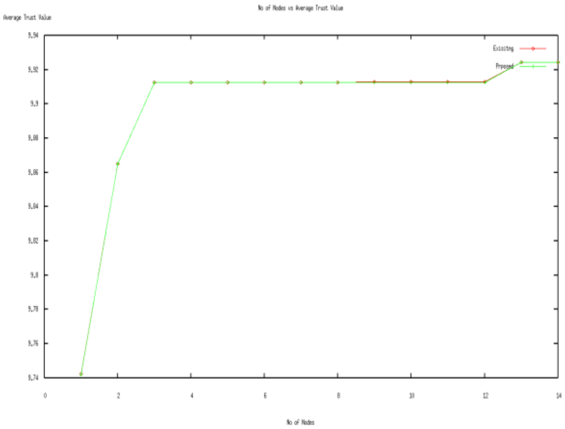

Fig 3: Number of Nodes Vs Average Trust Value

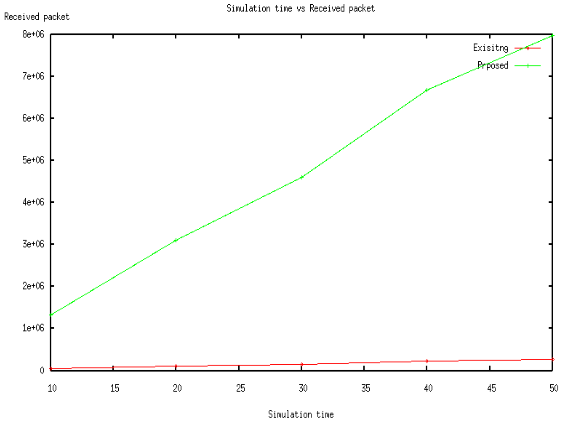

Fig 3: Simulation Time Vs Received Packets

VIII .CONCLUSIONS

From our work, conclude that the IDS in WSN can also be controlled by a leader as such as a regular node. Also this paper says that can control the resource utilization and time, cost. The cluster is elected basically by energy level of the nodes. This LBIDS give more performance of controlling IDS in WSN. The simulation result shows the performance of the proposed approach. The performance of the proposed system comparative with the existing system is given above.

REFERENCES

[1] Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET, Noman Mohammed, Hadi Otrok, Lingyu Wang, Mourad Debbabi, and Prabir Bhattacharya, Fellow, IEEE,VOL. 8, NO. 1, JANUARY-FEBRUARY 2011.

[2]Akyildiz LF,SuWL, Sankarasubramaniam Y, Cayirci E.“A survey on sensor networks”, IEEE Communications Magazine, 40(8):102~114, 2011.

[3] S. Bandyopadhyay and E. J. Coyle, “An Energy Efficient Hierarchical Clustering Algorithm for Wireless Sensor Networks”, in Proceeding of IEEE INFOCOM’03, San Francisco, April 2010.

[4] J. W. Branch, B. K. Szymanski, C. Giannella, R. Wolff, H. Kargupta, In-Network Outlier Detection in Wireless Sensor Networks,” in IEEE ICDCS’06, Lisboa, Portugal, July 2009.

[5] Inside Attacker Detection in Hierarchical Wireless Sensor Network, Yi-Ying Zhang, Wen-Cheng Yang, Kee-Bum Kim, Myong-Soon Park Department of Computer Science and Engineering Korea University, Seoul, Korea, © 2008 IEEE.

[6] I. Dace, An Introduction to intrusion Detection and Assessment, ICSA, Inc., Jan. 4, 2000.

[7] L. Garber, Denial-of-Service Attacks Rip the Internet,V. I’axson, S. Floyd, Wide Area Traffic: The Failure of Poisson Modeling, J. Beran, Statistics for Long Memory Processes, Chapman & Hall, 1994.

[8] M. Younis, M. Youssef, K. Arisha. “Energy-aware in Cluster based sensor networks”, in: Proceedings of the 10th IEEE/ACM International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS2002), Fort Worth, TX, October 2002, pp.129-136, (2002).

[9] S. Khan, K-k. Loo, T. Naeem, M.A. Khan, “Denial of service attacks and challenges in broadband wireless network,International Journal of Computer Science and Network Security, Vol. 8, No. 7, pp.1-6, July 2008.

[10] Y. Wang, G. Attebury, B. Ramamurthy, “A survey of Security issues in wireless sensor networks,” IEEE Communications Surveys and Tutorials, Vol. 8, No. 2, pp. 2-23, 2006.