Agent based secure intrusion detection and prevention for rushing attacks in clustering MANETs

A. Aranganathan1*, C.D. Suriyakala2

1Research Scholar, Satyabana Institute of Science & Technology, Chennai.
2Director, School of Ocean Engineering & Underwater Technology, Kerala University of Fisheries & Ocean Studies, Kerala.

*Corresponding author E-mail: aranganatee@gmail.com

Abstract

Intrusion detection is one of the challenging issues in wireless networks. The inherently vulnerable characteristics of wireless mobile ad hoc networks make them susceptible to attacks in spite of some security measures, and it may be too late before any counter action can take effect. As such, there is a need to complement security mechanisms with efficient intrusion detection and response systems. This paper proposes an agent-based model to address the aspect of intrusion detection in cluster based Mobile ad hoc network environment. The model comprises of mobile agents, which are used to detect intrusions, respond to intrusions, mainly preventing the routing attacks while securing them and distributing selected and aggregated intrusion information to all other nodes in the network in an intelligent manner to compensate the attack. The model is simulated to test its operation effectiveness by considering various performance parameters such as, packet delivery ratio, communication overhead, throughput. It implements a secure detection and prevention technique that contains the Blowfish algorithm which is a symmetric encryption and decryption algorithm having a secure standard till date against attack. Intrusion and meanwhile preventing it while focusing on the other constraints of the network. Agent based approach facilitates flexible and adaptable security services. Also, it supports component based software engineering components such as maintainability, reachability, reusability, adaptability, and flexibility.

Keywords: Mobile Ad hoc network, agent, intrusion detection system, malicious node.

1. Introduction

In MANETs, the scope of getting attacked increases by the malicious node which proves vulnerable to compromising of the data as well as the communication between nodes in the network architecture as the nodes being mobile in nature and having no centralized administration makes it prone to intrusion. In general the attacks in MANETs are classified into active and passive attack which are threat to the on going transmission as well as to the security of the system. The problem concerned here is the active attack which has always been proved fatal and causes a lot of security issues namely the black hole attack and the rushing attack which are major threat to the network, maintaining security and communication constraints simultaneously in the network is the sole target as this is the where the problem lies. Many systems has tried to control the attack but simultaneously failed maintaining the other constraints of the network. Detecting the intrusion and meanwhile preventing it while focusing on the other substantial properties of the network is the main area of concern in such active attacks as it affects the integrity of the system thereby reducing the performance of the overall system and it also compromises the transmission in between the communication scenario as these kind of attacks include any action that intentionally aims to cause any damage to the network as processing capability of the attacker is either wireless or wired and the number of attackers may be single or many. Agents are the autonomous or semi autonomous programs situated within an environment, which sense the environment and act upon it to achieve the goals. Some of the activities where this feature can be observed are: monitor the battery life, power requirements to neighbours, reliable neighbours, discover routes in anticipation to link breaks, checking intruders, studying legitimate user behaviour patterns, etc. This allows them to operate independently. The agent can react to changes in its environment such as changes in user behaviour, change in neighbours of a node, etc. anticipate the changes in the mobile ad-hoc networks environment and take appropriate decisions. An agent can be mobile, i.e., move from one place to another facilitating asynchronous communication between the nodes in MANETs.

Rushing attack

This uses duplicate suppression mechanism by which it quickly forward the route discovery reply to the routing request broadcasted in order to gain access to the forwarding data; the rushing attacker gain access in forwarding group and thus can tap data. The rushing attacker can make use of either quick forward request or quick reply to drop the data packets than normal nodes, thus the chances of selection of path that includes attacker increases.

Blowfish algorithm

Blowfish is a fast symmetric key method for both encryption and decryption of data. It encrypts data with a large 32-bit processor. The key is of variable from 32 to 448 bits. It makes use of simple all operations done by simple XOR, look up table with 32 bit key words.
2. Related works

Panos et al. [3] analyzed the effects of black hole attack focused on the route discovery process. This mechanism uses a dynamic threshold cumulative sum (CUSUM) test to detect abrupt changes in the normal behavior of AODV’s sequence number parameter against black hole attacks. A key advantage of the proposed mechanism is its ability to accurately detect black hole attacks with a minimal rate of false positives, even if the malicious node selectively drops packets. It is mainly focused on the false alarming during the monitoring of the malicious nodes and hence comprises in reducing it tracking the nodes.

Chowdhury and Neogy [5] define the mobile agent-based system (S) to be consisting of M independent agents deployed by k owners that may move in the underlying MANET. They develop a model that takes help of the abstraction of an ad hoc network. The nodes move according to Smooth Random Mobility Model and two ray propagation of radio signals is assumed while checking for link existence. Here they try to protect mobile agents from visiting malicious hosts (nodes) and to prevent trusted nodes from sending agents to malicious ones. They assumed the compromised nodes can send malicious agents to mislead a node about its trust level. Also a compromised node may work as a black hole to visit agents. In this scenario the mobile agent is taken as a token visiting one node to another in the network (if the nodes are connected) based on some strategy as needed by the underlying applications to accomplish its task. The model is based on priority list of agents, suspected list of nodes for agent, default trust level and trust view by the mobile agent for the initial nodes. The process is also designated taking the maximum number of nodes as well as maximum time an agent can be enrooted.

The model proposed by Reshma et al. [2] comprises of a set of static and mobile agents, which are used to detect intrusions, respond to intrusions, and distribute selected and aggregated intrusion information to all other nodes in the network in an intelligent manner. The model is simulated to test its operation effectiveness by considering the performance parameters such as, detection rate, false positives, agent overheads, and intrusion information distribution time. Agent based approach facilitates flexible and adaptable security services. Also, it supports component based software engineering components such as maintainability, reach ability, reusability, adaptability, flexibility, and customization.

Two Acknowledgement (TWOACK) based intrusion detection system proposed by Liu et al. [9] is used to avoid the collusion and limited transmission power by sending acknowledgment every transmission of data packets with two hops away from it from source to destination with three consecutive nodes. This scheme is based on predefined time period with two hops acknowledgment. Beyond the time period, it reported as a malicious node. Due to the battery limitation, the life span of the entire networks was degraded with redundant transmission process. The limitations of this scheme is that added network overhead for acknowledging every data packets.

Adaptive Acknowledgement (AACK) Scheme was implemented by Sheltami et al. [7] based on ACK based system mainly to avoid network overhead that source node simply sends data packets through the intermediate nodes to reach the destination node. After reaching the data packets at the destination, it will send the acknowledgement to the source node through the same route with reverse order. After receiving the ACK data packets from the destination node within predefined time period, the data packet transmission is successful from source to destination. This two ACK schemes (TWOACK & AACK) suffers by false misbehaviour report and forged acknowledgment packets. These are depends on acknowledgement of data packets but there is no guarantee for ACK data packets and node authentication.

Dasgupta et al. [6] proposed common intrusion detection security agent architecture to detect the intrusion in the system. Agent can monitor and to detect malfunctions, faults, abnormalities, misuse, deviations, intrusions, and provide recommendations (in the form of common intrusion detection language).

Emmanouil et al. [8] proposed an adaptive and secure routing protocol for eMANETs called ChaMeLeon (CML) for the purposes of emergency MANET routing supporting emergency communications. The objective of CML is the routing mechanisms adaptability towards changes in the physical and logical state of a MANET. CML outperforms both on reactive and proactive routing protocols by means of parameters includes average end-to-end data packet delay, cumulative delivery delay and cumulative packet jitter (which are crucial for multimedia streaming in eMANETs) while it has slightly increased control routing load. Additionally, they applied IPSec on top of CML to provide confidentiality, authentication and integrity to the transmitted packets.

The algorithm proposed by Tyagi and Dembla [4] detects black hole attacks and prevents it by using PUSH and POP operations. The source node uses additional information known as pseudo reply packet (PRREP). The node source stores the information about all the incoming packets in a look-up table designated as RREP_T. This table stores the PRREP sequences, arranged in ascending order using PUSH and POP operations. Any abnormality in the sequence is considered to be a PRREP sequence received from a malicious node and is discarded by the source. Furthermore, the table is periodically updated, with all the PRREP sequences stores for a set duration defined by STR_dur. A header node attached to each message received from different nodes, assigns a priority to the PRREP message and is considered in that order by the source node. The priority is calculated based on the sequence number, and the shortest sequence number is given the highest priority. Node having abnormal sequence number is considered as a malicious node and source broadcast this message in network. The network parameter mainly depends on the sequence number obtained while monitoring the network for malicious nodes.

Zhiua et al. [1] proposed an intrusion detection system based on dynamic state context and hierarchical trust in WSNs is proposed, which is flexible and suitable for constantly changing WSNs characterized by changes in the perceptual environment, transitions of states of nodes, and variations in trust value. A trust of both sensor nodes (SNs) and cluster heads (CHs) considers honesty trust, and content trust is put forward, which combines direct evaluation and feedback-based evaluation in the fixed hop range. That the trust of SNs is determined by CHs and the trust of CHs is evaluated by neighbor CHs and BS; in this way, the complexity of evaluation is reduced without evaluations by all other CHs in networks. Intrusion detection based with self-adaptive dynamic trust threshold, which improves the flexibility and applicability and is suitable for cluster-based WSNs.

The system proposed by Gajendra and Rajul [10] uses a technique for Rushing attack prevention which is done by calculating threshold time and average time and comparing it with request time. The AODV protocol is studied here and the parameters are monitored constantly over the network and the activities of the nodes are compared to a specific set of constraints that contain the log time for the activity of a predefined malicious attacker which in result is checked over and therefore marked as a compromised node.

3. Proposed system

The main objective of this paper is to create a system to detect the suspicious activity from the unsigned/ malicious nodes in the network and to prevent the nodes from making changes in the system by compromising the routing protocols, nodes and simultaneously preserving other constraints of the network to maintain the data transmission, the overall performance of the network and especially the communication in between the nodes and clusters in the network safely. The purpose of the work is also concerned with the other parameters of the network which
includes reducing the delay, packet loss and better packet delivery ratio.

**Intrusion detection and prevention**

In the secure detection and prevention (SDP) scheme, when the transmission starts the initial cluster heads are selected based on the energy and trust levels, these cluster heads form their cluster combining member nodes by sending them request as forming a dynamic cluster network which is mobile in nature as well as send the data of the member nodes to the mobile agent which compares the value with a specific threshold limit. If the node is found to be having an energy level more than the threshold limit it is marked as a malicious node and if the node posses an energy level less than the specific threshold limit then it is marked as a compromised node. The relative data figure out the presence of black hole node. Since the process on goes due to the monitoring activity of the agents it finds out the malicious node and changes the cluster network eliminating the dangerous nodes as it is dynamic in nature and the dynamic abilities changes subsequently while maintaining the data security & transmission protocol and hence by this way the proposed system is able to tackle with the black hole attack. Relating to the rushing attack when such instance is found out of manipulating the RREP the path of transmission immediately changes to a different source and destination so as to avoid the hop relay through the path of transmission as the rushing attacker tries to manipulate the RREP by making duplicate suppression so to prevent this the identity of source, destination node and the path of transmission is changed effectively against the presence of the attacker. In this way the transmission protocol and the data have been secured, the attacks has been detected and prevented which is carried out in the further simulation. It enhances the process by saving the routing protocols of the current path of transmission and yielding a better immunisation against the attacks. Thus the SDP method achieves over the intrusion activity and performs the prevention.

In the execution of the intrusion detection and prevention process takes place which includes the blowfish algorithm which is a symmetric encryption and decryption process and holds on the transmission from the source to the destination. It is embedded with hashing technique to make it faster for transmission and also makes it more secure yet effective against attacks from the malicious nodes. The mobile agent performs the remote work to determine the malicious node and shift the path of transmission in case of any compromised node in the network thereby making the network efficient and secure overall.

4. **Simulation results and discussion**

The simulation the process takes place in a sequential manner starting with the insertion of the nodes which includes both the member nodes and the malicious nodes in the network and enabling the transmission through the network. In this process a simple encryption and decryption process has been embedded along with the mobile agent.

The execution takes place and the transmission takes place with few packet drops and it displays the transmission range malicious nodes in it too. The execution takes place with the circles around the nodes transmission range of each of the nodes with the given simulation parameters as shown in table 4.1.

| Table 4.1: Simulation Parameters |
|-----------------|-----------------|
| No of nodes     | 50              |
| No of packets sent | 271             |
| Pack. Packets delivery ratio | 95.23           |
| Dropping ratio  | 7.01107         |
| Average Energy consumption | 8.65            |
| Delay           | 1.34            |
| Throughput      | 14.56           |
| No of packets dropped | 19              |
| Normalized routing overhead | 7.1547         |
| Jitter          | 0.36722         |
| Control Overhead| 2.47            |
| Routing Protocol| AODV            |

Figure 1 shows the complete cluster formation for all three groups with their respective cluster heads which is node 15 for cluster 1, node 18 for cluster 2, node 7 for cluster 3, node 26 for cluster 4 and along with their respective mobile agents mentioned and marked in the same colour as of the clusters and the attacker node is marked with red colour. The sequence of the operation continues with the existence of the attacker due to which the cluster management is carried through the random clusters and by the help of mobile agent to prevent the attack from compromising the nodes, transmission and information.

**Control overhead**

Here we can see a lesser control overhead which indicates a better network control operation including the scheduling, resource allocation, routing and flow control. The network control tasks necessitate the exchange of information regarding the network state, reduced overhead results in better efficiency as shown in figure 2.

**Packet delivery ratio**

Here we have achieved better delivery ratio of the message or packets when compared to the previous method. The packet delivery ratio is the ratio of the number of packets sent to the no of packets received with respect to the nodes. The packet delivery ratio is achieved at 95% in figure 3.
Key exchange

The key exchange is higher than the existing system which indicates a better network security or cryptographic operation throughout the process between the nodes. The audit based network performs the exchange maximum no of times when the respective nodes are present making the process more secure. The blowfish encryption algorithm takes 32 bits of key value as shown in figure 4.

Network throughput

From the figure 5 we can observe a better network through put in case of the implemented system which indicates a higher number of data transmission and operation throughout the process at 14Kbps when compared to the previous session at 10 Kbps. Hence a better throughput is achieved in the network.

5. Conclusion

Security is nowadays, a growing concern in everyone’s mind. Routing protocol is one of the points to be addressed. Security in mobile ad hoc networks is difficult to achieve, notably because of the vulnerability of wireless links, the limitation in the physical protection of nodes, the dynamically changing topology, the absence of a certification authority, and the lack of a centralized monitoring. Earlier studies MANETs aimed at proposing protocols for some fundamental problems, such as routing, and tried to cope with the challenges imposed by the new environment. These protocols, however, fully trust all nodes and do not consider the security aspect. They are consequently vulnerable to attacks and misbehaviour.

Due to the decentralised nature of MANETs, nodes must forward packets towards a destination by following the principles of a MANET routing protocol. To tackle with this issue a secure detection and prevention method is applied to detect the malicious nodes and to save the communication between the nodes by preventing the route disruption in a way in which the route discovery process is shifted from the path of transmission such that the loss is controlled and can be reduced to an higher extent. The method kicks in quickly to mitigate the path of transmission thereby saving the nodes as well as the data throughout the transmission. The further work can be extended considering the presence of a huge number of nodes in which less number of key is used for high security, an efficient detection algorithm can be implemented to further reduce network overhead problem.

References

[1] Zhang Z, Zhu H, Luo S, Xin Y & Liu X, “Intrusion Detection Based on State Context and Hierarchical Trust in Wireless Sensor Networks”, IEEE Access, Vol.5, (2017), pp.12088-12102.
[2] Reshmi BM & Manvi SS, “An agent based Intrusion Detection model for mobile ad hoc networks”, Mobile Information Systems, Vol.2, (2006), pp.169–191.
[3] Panos C, Ntantogian C, Malliaros S & Xenakis C, “Analyzing, quantifying, and detecting the blackhole attack in infrastructure-less networks”, Computer Networks, Vol.113, (2017), pp.94-110.
[4] Tyagi P & Dembla D, “Performance analysis and implementation of proposed mechanism for detection and prevention of security attacks in routing protocols of vehicular ad-hoc network (VANET)”, Egyptian Informatics Journal, Vol.18, No.2,(2017), pp.133-139.
[5] Chowdhury C & Neogy S, “Securing Mobile Agents in MANET against attacks using Trust”, International Journal of Network Security & Its Applications, Vol.3, No.6,(2011).
[6] Dasgupta D, Gonzalez F, Yallapu K, Gomez J & Yarramsetti R, “CIDS: An agent-based intrusion detection system”, Computers & Security, Vol.24, (2005), pp.387-398.
[7] Shakshuki EM, Kang N & Sheltami TR, “EAAK: A Secure Intrusion Detection System for MANETs”, IEEE transactions on industrial electronics, Vol.60, No.3, (2013).
[8] Panaousis EA, Ramrekha TA, Millar GP & Politis C, “Adaptive and secure routing protocol for emergency mobile ad hoc networks”, International Journal of wireless and mobile networks (IJWMN), Vol.2, No.2, (2010).
[9] Rau K, Deng J, Varshney PK & Balakrishnan K. “An acknowledgment-based approach for the detection of routing misbehaviour in MANETs”, IEEE Trans. Mobile Computing, Vol.6, No.5, (2007), pp.536–550.
[10] Chandel GS & Chowksi R, “Study of Rushing attack in MANET”, International Journal of Computer Applications, Vol.79, No.10,(2013).