Middle-East Journal of Scientific Research 25 (11): 1954-1957, 2017
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2017.1954.1957

A Novel Approach of a Secure Intrusion Detection Systems in ad-hoc Wireless Networks Using Software Agents

[1]A. Aranganathan and [2]C.D. Suriyakala

[1]Research Scholar, Sathyabama University, Chennai, India
[2]Director, Kerala University of Fisheries & Ocean Studies, Kerala, India

Abstract: Ad-hoc wireless networks is a set of nodes are movable which are communicating with each other. Each node acts as a router can forward the packets through intermediate nodes from source to the destination path. The main problem of ad-hoc wireless networks has no predefined infrastructure and also with dynamic topology. Malicious node is the severe attack in wireless ad-hoc networks which affects the performance such as long delay, less throughput, out of time packet end to end delivery, packet overhead, path in optimality. Many researchers have been developed the detection techniques against the malicious attacks. In this paper, analyze the detection of malicious nodes using software agents and also to secure these agents with ECC (elliptic curve cryptography) with digital signature algorithm compares with the existing secure intrusion detection systems like TWOACK, EAACK with digital signature schemes to improve the security of the networks such as packet delivery ratio, routing overhead and end to end delay using network simulator tool.

Key words: Software agents · ad-hoc wireless networks · Malicious node · Intrusion detection

INTRODUCTION

A wireless ad hoc network is a multiple number of movable nodes connected by wireless radio link connected with data packet. All the movable nodes are freely to move in a random direction.Nodes may leave or join within the network coverage called dynamic changing topology. It is a decentralized type of wireless network. In wireless ad-hoc networks is of two types namely single hopping and multiple hopping. Single hopping is the communication between the two nodes within the same radio range. Multi hopping means using intermediate nodes can communicate the information from source node to the destination node. Intermediate nodes can acts as a forwarder. These networks used for emergency applications like rescue and fire-fighting, military environments like soldiers, tanks and also for personal area networks like cell phone, laptop. The main drawbacks of wireless networks is loss of packets due to transmission errors, frequent disconnection, short battery lifetime, limited capacities, possibility of malicious nodes acts as a trusted nodes in the networks called as attackers or intruders that can disturb the normal functioning of the network activities in different routing protocols called intrusion. This plays the challenging role for security issues in wireless networks will be discussed in the next section.

There are two basic routing protocols in wireless ad-hoc networks namely proactive and reactive routing protocols. The proactive routing protocols maintaining the routes in a established path with less delay and also keep the routing information can be updated with more bandwidth consumption and more network overhead. The reactive routing protocol is based on demand basis. The routes are established on request using RREQ and RREP with less overhead. The drawback in this protocol is more delay is needed for establishing the route. The famous routing protocol is AODV, DSDV and DSR. In this paper, DSR protocol is implemented.

Related Works: Malicious node is the node which can degrade the performance of the systems. The basic types of malicious attackers (intruders) are active attackers and passive attackers, Active attackers are dangerous networks which directly disturbs the normal network functions such as injecting, altering and modifying the data packets. Passive attackers are the intelligent attacks without changing the data packets; its operation is not

Corresponding Author: A. Aranganathan, Research Scholar, Sathyabama University, Chennai, India.

affected by these attacks. There are various active attacks namely spoofing attacks, blackhole attacks, greyhole attacks, wormhole attacks.

Intrusion detection is the more challenging task in wireless networks compares with the fixed networks, because in wireless networks have no security, no base basestation.So the possibility of malicious nodes can attacks the true nodes. Intrusion detection is to monitor the activities of the entire node, detect the malicious nodes to identify which node is malicious and also inform to the neighboring node to avoid the malicious node.

To avoid this problem, some of the intrusion detection systems had been developed to detect the activities of the malicious nodes such as watchdog, pathrater, TWOACK; Adaptive acknowledgement (AACK).Watchdog is nothing but to watch the node behavior of the next hop's transmission. If the next node not able to forward the packets within the threshold time, it increases the counting number. The drawbacks of watchdog in the presence of malicious nodes is limited power, collisions, partial dropping and false misbehavior report. TWOACK is based on acknowledgement method. It detects the malicious nodes by transmitting data with acknowledgement for every consecutive three nodes from source to the destination path called two hopping method. Along the same path the acknowledgement should be received back to the source within the specific time period, otherwise it reported as a malicious node. The drawbacks of TWOACK scheme are degrading the lifespan of the battery power by sending and receiving ACK for two hopping only. EAACK, an enhanced adaptive acknowledgement scheme implemented with digital signature for guarantee of valid acknowledged data packets with malicious reports authentication (MRA) to the source. The limitation of the scheme is securing a digitally signed data with more network overhead. To improve the security of the network, software agents are implemented.

Software Agents: Software agents are not only able to move from one node to another node for collecting the information but also the capability to interact with the environment. Software agents are the agents which are mobile and static agents. Mobile agents can move and collect the information about the routing path, traffic congestion, energy level of each node and its returns to a static agent. Benefits of novel routing scheme has some advantages like maximize network performance, scalability, less delay, end to end reliable communications and minimize losses.

Mobile agents get resources from all the node and passing all these information to the static agent which has stationary node locating at the central point for data access. Mobile agents can collect the data transparently to the nodes. Wireless network agents are well equipped to observe the evolution of the network, any sudden connection/disconnection of a roaming node. This leads to better routing of the information.

Some of the characteristics of the agents are:

- Agents must be able to react to changes in its environments, such as change of users, change of network connections.
- Agent can work without the requirement of a central server. This allows them to operate independent even if there is a lack of network connection.
- Agent has a single task like monitoring of user login, monitoring user behavior. Agents interact with themselves and adapt themselves.
- Agent should be able to stop its execution and start it again from the same point.
- Agents must be able to communicate with others, possibly server.
- Not possible to upgrade an agent on regular basis once they deployed, agents should try and learn from its own experience.
- Mobile agent can autonomously move from host to host, access local resources through communication channels with stationary agents.
- Agents reduce network load, reduce network latency

Proposed System: In this paper, a trusted centralized agent (TCA) and trusted mobile agent (TMA) has been implemented to find out the malicious node (faulty node).Mobile agent is used to track all the node behavior in the network and it detects which node is malicious. Trusted centralized agent is a stationary one which stores all the nodes information in the memory and also listing out the malicious node that synchronizes with the mobile agent for data communication. With the help of the mobile agent, packets are received to the destination in a secured manner. If any attackers entering the networks, mobile agents in different paths reports to the trusted centralized agent. The centralized agent put under block list for not sending or receiving from the attacker's node.

Elliptic curve cryptography (ECC) is a part of public key cryptography with twice the size of the security level in bits with minimum key size compared to the key size of DSA. Suppose Alice wants to send a digital message (m) to Bob with the following steps.

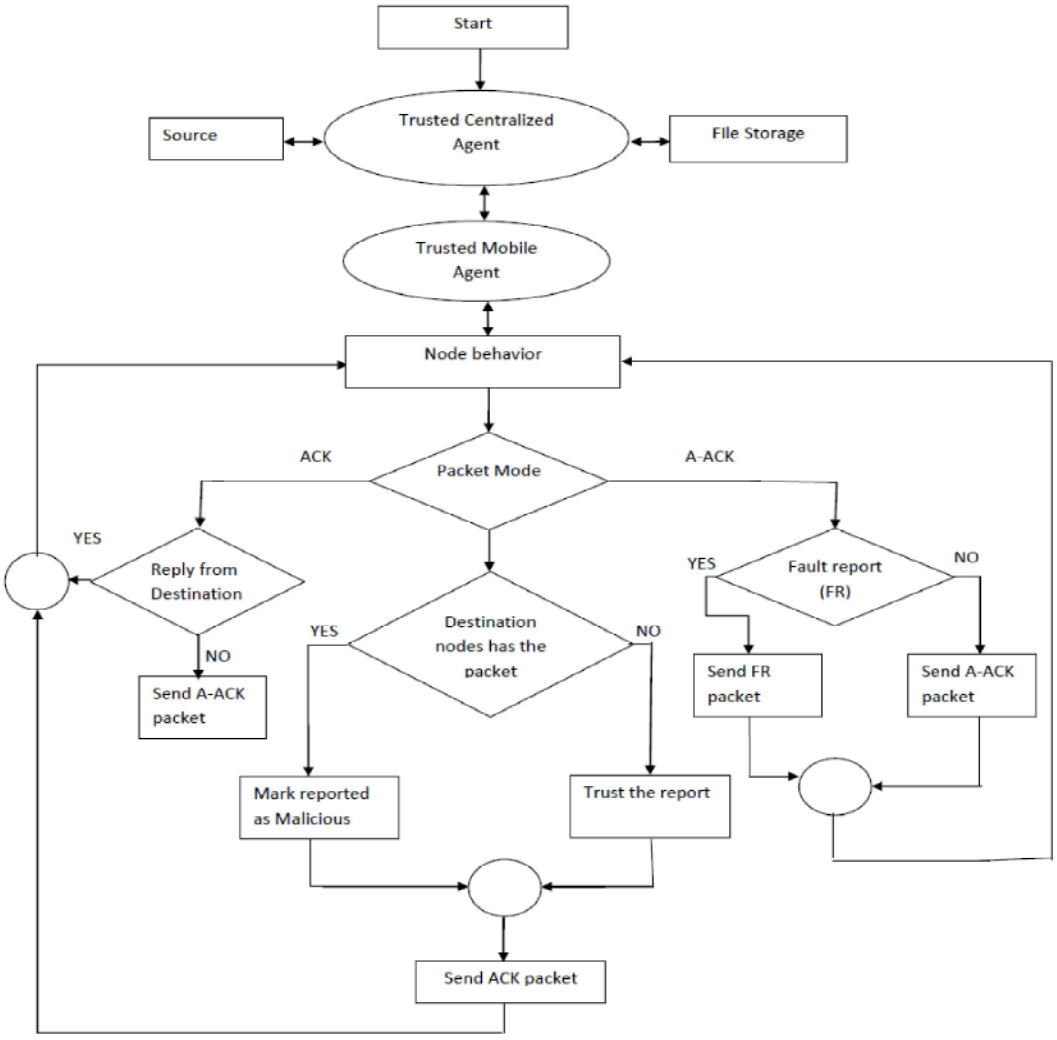

Fig. 1: Agent based secure intrusion intrusion detection system (A-SIDS)

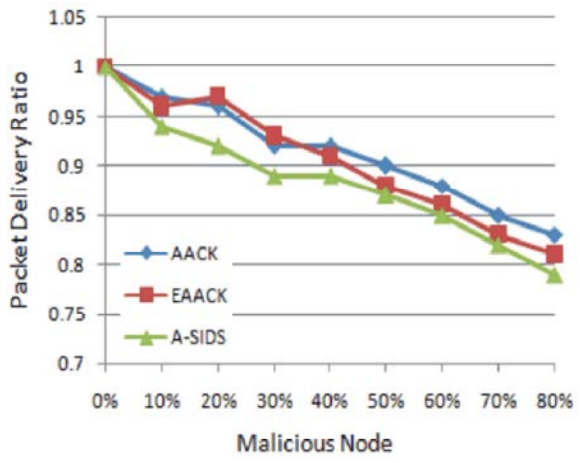

Fig. 2: Packet delivery ratio

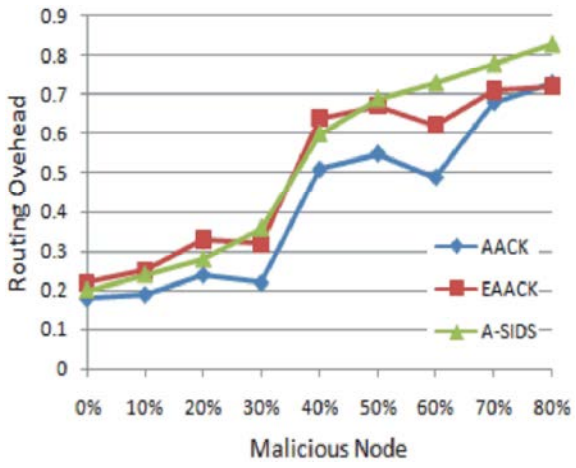

Fig. 3: Routing overhead

Simulation Results and Discussion: To compare the performance metrics of a proposed agent with secure detection methods with the previous acknowledgment based schemes such as EAACK and TWOACK.Some of the parameters has been taken for consideration.

Packet Delivery Ratio (PDR): It is nothing but the number of data packets received to the number of data packets transmitted. In this paper, packet delivery ratio of agent based secured intrusion detection is improved when comparing with existing acknowledgement based EAACK and TWOACK.

Routing Overhead (RO): It is related to request and reply based schemes like RREQ, RREP and RRER. Agents can take care of some agent based authenticated acknowledgment packets (A-ACK) instead of sending every time to the each node. So that routing overhead can be reduced by monitoring all the node behavior activities within the network.

End to End Delay: The timing to reach the packets to the destination is being calculated from source to the destination by trusted a mobile agent which is communicated with centralized trusted agent. Suppose if the packets are affected with malicious nodes or node delay or any broken line that can quickly intimated to the centralized agent. Centralized agent blocks list the attackers node. In that way, end to end delay can be reduced.

CONCLUSION AND FUTURE WORK

Denial of service attack is the major drawback in the wireless ad-hoc networks. To avoid that, a proposed authenticated agent with secure intrusion detection systems(A-SIDS) with elliptic curve cryptographic techniques was implemented for securing the agents for securing the data transmission overcoming of existing systems like EAACK and TWOACK schemes. Future, we can test this performance in real time implementations and also with ECC based algorithms like Diffie-Hellman scheme.

REFERENCES

1. Akbani, R., T. Korkmaz and G.V.S. Raju, 2012. Mobile Ad hoc Network Security, in Lecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, pp: 659-666.
2. Akbani, R.H., S. Patel and D.C. Jinwala, 2012. DoS attacks in mobile ad hoc networks: A survey, in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, pp: 535-541.
3. Anantvalee, T. and J. Wu, 2008. A Survey on Intrusion Detection in Mobile Ad Hoc Networks, in Wireless/Mobile Security. New York: Springer-Verlag,
4. Kang, N., E. Shakshuki and T. Sheltami, 2010. Detecting misbehaving nodes in MANETs, in Proc. 12th Int. Conf. iiWAS, Paris, France, pp: 216-222.
5. Kang, N., E. Shakshuki and T. Sheltami, 2011. Detecting forged acknowledgements in MANETs, in Proc. IEEE 25th Int. Conf. AINA, Biopolis, Singapore, pp: 488-494.
6. Liu, K., J. Deng, P.K. Varshney and K. Balakrishnan, 2007. An acknowledgment-based approach for the detection of routing misbehavior in MANETs, IEEE Trans. Mobile Comput., 6(5): 536-550.
7. Patwardhan, A., J. Parker, A. Joshi, M. Iorga and T. Karygiannis, 2005. Secure routing and intrusion detection in ad hoc networks, in Proc. 3rd Int. Conf. Pervasive Comput. Commun., pp: 191-199.
8. Singh, A., M. Maheshwari and N. Kumar, 2011. Security and trust management in MANET, in Communications in Computer and Information Science, New York: Springer-Verlag, 147(3): 384-387.
9. Nasser, N. and Y. Chen, 2007. Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network, in Proc. IEEE Int. Conf. Commun., Glasgow, Scotland, pp: 1154-1159.
10. Parker, J., J. Undercoffer, J. Pinkston and A. Joshi, 2004. On intrusion detection and response for mobile ad hoc networks, in Proc. IEEE Int. Conf. Perform., Comput., Commun., pp: 747-752.