APTIKOM Journal on Computer Science and Information Technologies
Vol. 3, No. 1, 2018, pp. 1~5
ISSN: 2528-2417
DOI: 10.11591/APTIKOM.J.CSIT.79

Intelligent agents based trusted revocation for securing clustering MANETS

A.Aranganathan*[1], C.D.Suriyakala[2]
[1]Department of Electronics and Telecommunication Engineering, Faculty of Electrical and Electronics, Sathyabama University, Chennai-600 119, Tamil Nadu, India
[2]Kerala University of Fisheries & Ocean Studies, Kerala, India
*Corresponding author, e-mail: arangaece@gmail.com

Abstract

Mobile Ad-hoc Network is a non-secure wireless network which has no infrastructure, dynamical topology in which the nodes can move anywhere, may join or leave the network through multi-hop communication. In cluster network, all the nodes can select one Cluster Head for transmission of data to another Cluster Head through gateways which is mainly used for saving energy of each node. Intelligent agents are used for collecting secure data from neighboring nodes and inform to the trusted agent in clustered networks. Security plays major role in wireless medium. Detecting malicious node is also causing a major concern to damage the data packets. To avoid this problem of entering malicious node in networks and non-secured data, agents based trusted revocation in clustering mobile ad-hoc network for improving security with Certificate Authority to improve the network performance like high throughput, less latency time and improved certificate revocation time using ns2 simulators.

Keywords*: certificate revocation, cluster head, cluster, intelligent agents*

1. Introduction

A mobile ad hoc network is a wireless ad -hoc network which comprises of number of nodes which are movable from one end to another. In mobile ad hoc networks has no infrastructure facility for authorizing trusted and non-trusted nodes. Mobile nodes can freely move anywhere and it may join or leave the network. So there is no guarantee of malicious free nodes between two nodes. Mobile ad hoc network is used for military, commercial, emergency situations and other private applications. The main challenges in ad hoc networks are vulnerable to malicious attacks and other challenges include network power sources, bandwidth limitations, scalability and mobility. There are many research areas such as quality of service, security, routing, intrusion detection and route maintenance of the network. Intrusion detection and prevention of malicious node is the main challenging than fixed network. Intrusion detection is to detect the malicious nodes in the networks. Malicious node is nothing attacks that the unwanted sending of false data packets to the neighboring node, not forwarding original data packets to the destination called packet dropping. There are many types of attacks basically namely active and passive attacks. Other types of attacks are routing attacks namely Black hole attack, Grey Hole attack, Sleep Deprivation attack, Flooding attack, Rushing attack, Sybil attack, Worm Hole attack. There are many methods proposed for detecting malicious attacks namely watchdog and path rater, TWOACK, AACK, EAACK intrusion detection based approaches [1-6].

Routing is the challenging protocol for conveying the information from one path to other path through selective forwarding of intermediate nodes. In MANETs design, packet routing is the major problem. Routing algorithm has three basic approaches for routing of packets namely proactive routing, reactive routing and hybrid routing. Proactive routing protocol conveys routing data packets information through nodes actively by updating routing table and also allows any source to immediate routing to the destination (eg., Destination Sequenced Destination Vector, Wireless Routing Protocol). Reactive routing protocol (Dynamic Source Routing, Ad-hoc On- demand Distance Vector Routing) is a bandwidth efficient on demand routing protocol which has two routing functions namely route discovery and route maintenance. Route discovery is responsible for finding and establishing a new route to reach destination with multi-hop schemes. Route maintenance is responsible for detecting link breaks and repairing existing route and also finds an alternate route to minimize network overhead. Clustering in mobile ad hoc network

Received November 9, 2017; Revised February 1, 2018; Accepted February 10, 2018

plays a vital role for improving network performance and resource management. In clustering method [7], many numbers of mobile nodes are forming as a group. Each mobile node has a different behavior that performs indidual function such as cluster Head (CH), cluster Gateways or cluster member. Cluster Head have some characteristics such as node energy level, distance and received signal strength of a node, worked as an intra-cluster communication. Cluster Gateway performs inter-cluster communication between two CH. Cluster member is nothing but the group of nodes (not a CH) without any inter- cluster transmission as shown in the Figure 1.

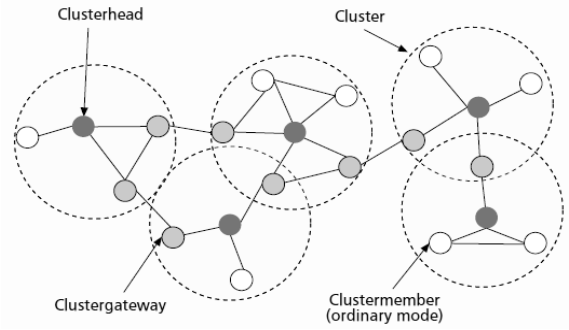

Figure 1. Cluster formation arrangement

2. Related Works

Wei Liu at al [1] proposed a cluster based certificate revocation with vindication capability for improving the accuracy and reliability of legitimate nodes using threshold mechanisms to make secure communication against malicious attackers. According to node reliability, there are three categories in this scheme namely normal node, warned node and revoked node. Normal node with high reliability to send data packets to the neighboring node and it may act as a cluster member or cluster head. Warned nodes have some restrictions for communicating data packets with its neighbor's node. It is a low reliability node with a combination of legitimate nodes and few malicious nodes. Revoked nodes with little reliability can acts as malicious nodes. Certification authority is for monitoring the nodes behavior and is used for updating warned list and black list of malicious nodes.

The scheme proposed by W.Liu et al [2] proposed a cluster based certificate revocation method performs revocation certificate of malicious nodes perfectly by threshold mechanism for protecting legitimate nodes from the attackers. Clustering networks mainly for detecting false accusations using certificate recovery packet method. This method is mainly for detecting whether the cluster head is malicious or not by keep on broadcasting certificate authority to all the cluster heads. Three categories of nodes are normal nodes, warned nodes and attacker nodes. Certificate authority maintains blacklist and warning list. Antesar M et al [3] proposed the scheme for filtering out malicious nodes for improving packet delivery ratio with multi-hop intermediate nodes. The proposed method analyses the functions of both recommendation managers which is an intermediate between indirect trust computation and cluster manager components. Recommendation manager sending request for neighbor's node behaviors' and gathers information about the node activities. Clustering manager maintains filtering algorithm for trustworthy nodes. The recommendation method showed the results for improving throughput and packet loss against untrusty nodes comparing with existing methods. Saurabh Sharma & Sapna Gambhir [4] proposed the method for detecting and removal of malicious nodes by using cluster and reputation based schemes in mobile ad-hoc networks. This scheme cluster head should maintain three tables namely legitimacy table, reputation table and neighbor table for keeping all the node information which is done by AODV reactive routing protocol.

J.-H. Cho et al [5] a trust management scheme was developed for mobile ad-hoc networks. The main focus of the trust scheme is to make security policies and other relationships. Trust management involves secure routing, intrusion detection, access control, authentication and key management. Secure routing is for detecting malicious nodes behavior and also adds trust values. Many researchers described the trustworthy schemes such as watchdog, path rater by AODV and DSR protocol. Intrusion detection system (IDS) is nothing but the authorized nodes can detect malicious nodes locally to make security. The well behaving nodes have a right access to share network resources using. localized trust group.

Authentication is mainly for establishing trust relationship like calculation of weight trust based on the distance. A key management scheme provides many security establishments between the nodes such as modified hierarchical public key infrastructure with high service based on security association.

Trust management plays a vital role in distributed environments. There are two major security mechanisms in MANETs. One is pre-configured and another is self-organized security mechanisms. Distribute Certificate Authority (DCA) in mobile adhoc networks based on threshold methods with improved trust models but the networks need prior configuration. I t is very difficult to get MANET characteristics like dynamic topology, temporary networking is needed. This is not the guarantee of network availability and also overload. The features of self-organizing mechanisms need self building networks are opted for mobile adhoc environments [8]. Another one is certificate chain (CC) based on Public Key Infrastructure (PKI) and trust is based on true relationship between the nodes. CC based security mechanism mainly avoids the limitations of DCA. The theme of CC is to maintain the true relationship by transmitting certificate chain. The advantage of using CC is to maintain trust relationship without centralized or distributed trust center. The limitation has to maintain large certificate map by adding more number of nodes in the network. By avoiding these limitations by introducing availability of MANET to be analyzed. There are different security attacks namely attacks against integrity, attacks against confidentiality and attacks against availability. In black hole attack, the packet loss can be occurred and not delivering of data packets to destination. Security trust model is to evaluate the node is used for reliability of message. The aim of security trust model is to respond the request promptly, transfers and delivers the data packets to the destination promptly. Safety trust model is nothing but all the data packets in the networks are transferred by data packet pattern and also it complies with network behaviors and certain trusted nodes are correctly delivering the data packets promptly. Negative trust model means that not promptly transfer and delivery of all the data packets. Web collaboration trust is by node created trust based systems with collaboration ability to transfer data within specific time period. Stand-alone trust is to transfer stand-alone efficiency trust value from certain node to another node.

Many researchers have been proposed for mitigating attackers in the networks. Certification is acting as a primary role for removing malicious nodes from the network and cut off them all the activities immediately [9]**.** Certificate Authority manages certificate for all the nodes. There are many steps involved in the certificate revocation namely network creation, certificate creation and storing, broadcast certificate, profile table request, certificate revocation and copying false accusation. Matija Capan [10] proposed agent controlled mobile ad-hoc network, that the moving of faster nodes is difficult to find the stable path from source to destination if the two nodes are far apart, then RREQ messages are not able to find the way to the destination. Speed nodes form small cluster has no connectivity. To make connectivity, every cluster should have one or two backbone networks depend on the cluster size. Agents can be communicated directly in many ways such as point to point, broadcast. Sometime agents can be acts as a indirect ways for getting information by changing the environments.

3. Proposed System

Due to dynamic nature of topological wireless mobile ad-hoc networks is a challenging task for secure routing. There is a chance of dropping data packets by various routing attacks to reduce the performance of networks in a non-secure manner. The way to protect the network against packet dropping attacks. Many researchers had been developed cryptographic algorithms for securing networks high time delay with high cost. In the proposed scheme, implementing agents based trust certificate revocation for securing Cluster Head and cluster members from packet dropping attack source to destination in Zone Routing Protocol (ZRP) is a hybrid routing protocol, hierarchical networks for node energy conservation. An agent model consists of two agents are ii) Mobile agent and ii) Trusted agent (Static agent). Mobile agent which collects all the information of each cluster node energy level and their location also. Based on their energy level, mobile node only elects the Cluster Head. Mobile agents broadcasting RREQ to their neighboring nodes and wait for their response within specified time period. Within the specified time, each node has to send RREP to the mobile agent for further communication to reach the destination. Otherwise, the node can be assumed as a malicious node. After getting reply from the neighboring nodes, mobile agent sends signed certificate revocation can be issued to the nodes. For those information can be updated to the trusted agent. If any changes in delay of nodes, further mobile agents have to check with trusted agent for verification. Then only the data packets can be reached to destination for improving high performance metrics like high throughput ratio, less certificate revocation time and less packet latency when compare with existing approach of certificate trust based revocation.

Table 1. Simulation Parameters

Parameter	Value
No of nodes	50
Network Dimension	1000 m*1000 m
Simulation time	400 sec
Routing protocol	Zone Routing Protocol
Cluster update time interval	10s
No. of malicious nodes	3
MAC protocol	IEEE 802.11
Mobility model	Random waypoint
Speed	10-100m/s

4. Results and Discussion

Agent based trusted revocation time changes with the number of attacker node between existing scheme and proposed scheme. Using trusted agent, the number of attacker nodes should be less than the legitimate nodes. So the number of trusted by agent for legitimate nodes are used to revoke attacker certificates. In Figure 2 shows that packet latency time using trusted agent based certificate can be reduced when compares the certificate revocation schemes to get improved performance of networks. In Figure 3 shows the improved revocation time with the implementation of threshold time given by mobile agents with the existing approach. From Figure 4 analyzed that there is a high throughput performance in the agent based approach by ensuring security of all the cluster nodes and Cluster Heads (CH) with updating information within the specified intervals, otherwise it assume it as a malicious node by the mobile agents in the proposed system.

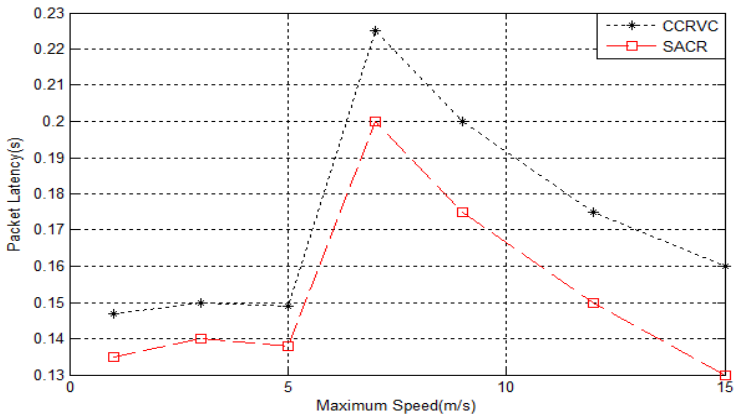

Figure 2. Packet latency time

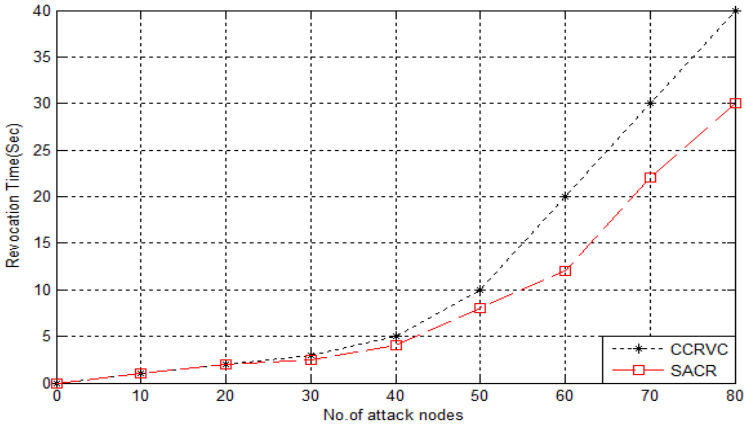

Figure 3. Reduced Revocation Time

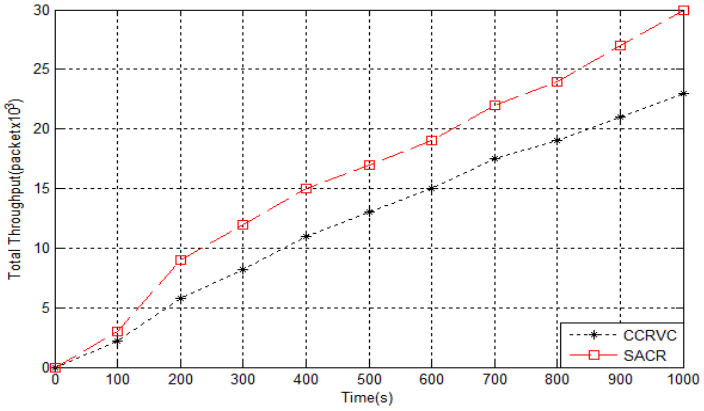

Figure 4. Throughput rate in trusted agents

5. Conclusion

In the proposed work, an implementation of agents based trusted certificate authority revocation scheme for ensuring the security against malicious nodes (attacks) especially in packet dropping attacks to improve the reliability of nodes, throughput and less packet latency time. Not only this attack, there are many types of attacks are in wireless ad-hoc wireless affects network degradation. So we have to use high level cryptographic methods to protect the nodes in clustering ad-hoc networks.

Acknoledgements

The researchers are grateful to SATHYABAMA UNIVERSITY for supporting this work.

References

[1] Wei Liu, Student Member, IEEE, Hiroki Nishiyama, Member, IEEE, Nirwan Ansari, Fellow, IEEE, Jie Yang, Nei Kato, Senior Member, IEEE. Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks. *IEEE Transactions on Parallel and Distributed Systems*. 2013; 24(2).

[2] W Liu, H Nishiyama, N Ansari, N Kato. *A Study on Certificate Revocation in Mobile Ad Hoc Network*. Proc. IEEE Int'l Conf. Comm. (ICC), June 2011.

[3] Antesar M Shabut, Keshav P Dahal, Senior Member, IEEE, Sanat Kumar Bista, Irfan U Awan. Recommendation Based Trust Model with an Effective Defence Scheme for MANETs. *IEEE Transactions on Mobile Computing*, 2015; 14(10).

[4] Saurabh Sharma, Department of Computer Engineering, National Institute of Technology, Kurukshetra, India, Sapna Gambhir, Department of Computer Engineering, YMCA University of Science and Technology, Faridabad, India. *RCMD&R: Cluster and Reputation based cooperative malicious node Detection & Removal scheme in MANETs*. Intelligent Systems and Control (ISCO), 2017 11th International Conference on 5-6 Jan 2017.

[5] J-H. Cho, A Swami, R Chen. A survey on trust management for mobile ad hoc networks. *IEEE Communication. Surveys Tuts*. 2011; 13(4): 562-583.

[6] Adnan Nadeem, Member, IEEE, Michael P Howarth. A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks. *IEEE Communications Surveys & Tutorials*. 2013; 15(4).

[7] Jane Y Yu, Peter H J Chong, Nanyang Technological University. A Survey of Clustering Schemes for Mobile Ad Hoc Networks. *IEEE Communication Surveys*. 2005; 7(1).

[8] Xibin Zhao, Zhiyang You, Zhifeng Zhao, Danning Chen, Feng Peng. *Availability based trust model of clusters for MANET*. 7th International Conference on Service Systems and Service Management, 2010.

[9] Jissmol Jose, Swapna B Sasi, Dept. of Comp.Science, Jyothi Eng.College, Thrissur, Kerala, India. *Certificate Revocation in MANET Using clustering*. IEEE Sponsored 9th International Conference on Intelligent Systems and Control (ISCO)2015.

[10] Matija Capan. *Self-organizing software agents for communication management in mobile ad hoc networks*. MIPRO, 2010 Proceedings of the 33rd International Convention, 2010.