Coalition Formation for Cooperative Packet Delivery in Hybrid Wireless Networks

S. Muthu Lakshmi, S. Manikandan
Department of Communication Systems, PSN College of Engineering and Technology, Tirunelveli, India

***Abstract*—*Hybrid wireless network (HWN) is an integrated infrastructure that provides seamless services over the several networks. In Hybrid Wireless Networks where adhoc and infrastructure based networks are used. The objective is to form a coalition structure by analyzing the behavior of each node present in the network for improved cooperative packet delivery. By applying Social Network Analysis (SNA) the computational complexity of coalition formation is reduced. The markov chain model is formulated to allocate the delivery path for each node present in the network and the coalition formation done by using voting mechanism. The packet delivery depends on the probability that each node will help other nodes in the same coalition. Bargaining game method is used to predict the optimum helping probabilities. For accurate certificate revocation Cluster-based Certificate Revocation with Vindication Capability (CCRVC) is used.*

***Keywords*— Adhoc network, BS oriented networks, Cooperative packet delivery, Hybrid wireless networks, Social network analysis.**

I. INTRODUCTION

Wireless networks and mobile host is widely available and popular. Wireless communications and network topology is the key to supporting a variety of applications such as safety and emergency notification. For such applications, which are provide through public wireless networks, base station(BS)/access points(AP) sporadically deployed across the roads act as the gateways between mobile nodes and other terrestrial networks for data communication. Wireless network have become attractive communication. Many cities and public places have deployed wireless networks to provide internet access to residents and local business. When the wireless link condition between the base station and a mobile node is poor carry and forward based cooperative data delivery will be useful to reduce the delay of data delivery. Intelligent transport system (ITS) architecture

Provides a collision free and effective data transmission to vehicular adhoc networks. It is provides public safety message delivery and multimedia communication to vehicular networks and road side users. The primary goal of the techniques is collision avoidance, route planning, and automatic tolling and traffic control. There are several methods has been proposed to achieved the above primary goals of ITS.

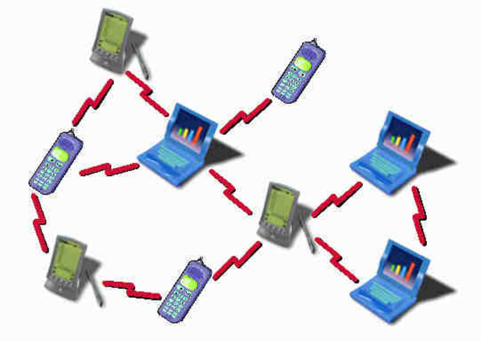

Fig.1 Adhoc Network

The provisioning protected communication between mobile nodes in a hostile environment in which a malicious attacker can launch attacks to disturb network security.

Fig.2 BS Oriented Network

In the vehicular networks there are no end to end path between the communications sources and destinations due to sparse node density and unpredictable node mobility. In such kind of networks, traditional ad hoc routing protocols, which relay on the end to end paths, fail to work. So it is necessary to maintain the end to end path between the communication source and destination. Security is one crucial requirement for these network services. Certificate management is a widely used mechanism which serves as a means of conveying trust in a public key infrastructure to secure application and network services. A complete security solution for certificate management should encompass three components: prevention, detection, and revocation. Certificate is a prerequisite to secure network communications. Certificate revocation is an important task of enlisting and removing the certificates of nodes that have been detected to launch attacks on the neighborhood. If a node is compromise or misbehaved it should be removed from the network and cutoff from all its activities immediately.

II. METHODOLOGY

2.1 VOTING BASED MECHANISM

Voting based mechanism is defined as the means of revoking a malicious attacker's certificate through votes from valid neighboring nodes. The certificates of newly joining nodes are issued by their neighbors. The certificates of an attacker are revoked on the basis of votes from its neighbors. In URSA, each node performs one-hop monitoring and exchanges monitoring information with its neighboring nodes. When the number of negative votes exceeds a predefined the threshold is much larger than the network degree, the nodes that launch attacks cannot be revoked and can successively keep communicating with other nodes. URSA does not address false accusations from malicious nodes. The weight of the node is calculated in terms of reliability and trustworthiness of the node that is derived from its past behaviors, like the number of accusations against other nodes and that against itself from others. The stronger its reliability, the greater the weight will be acquired. The certificate of an accused node is revoked when the weighted sum of voters against the nodes exceeds a predefined threshold.

Cluster based certificate revocation scheme, where nodes are self-organized to form cluster. A trusted certification authority is responsible to manage control messages, holding the accuser and accused node in the warning list and black list respectively. The certificate of malicious attacker node can be removed from the black list by its cluster head

The voting based mechanisms are the high accuracy in confirming the given accused node as a real malicious attacker or not. The decision making process for rapid certificate revocation as well as reduce the communication overhead the accuracy determine an accused node as a malicious attacker and reliability of certificate revocation will be degraded as compared with voting based method. The non-voting based method can revoke a suspicious misbehaved node by only one accusation from any single node with valid certification in the network.

Cluster based certificate revocation with vindication capability (CCRVC) scheme. The cluster head plays an important role in detecting the falsely accused nodes within its cluster and recovering their certificates to solve the issue of false accusation.

CCRVC inherits the merits of the non-voting based schemes it improving the reliability and accuracy as compared to the non- voting based scheme. CCRVC can quickly revoke the malicious device's certificate, stop the device access to the network and enhance the network security.

2.2 MODEL OF FUNCTION

The cluster based revocation scheme which can quickly revoke attacker nodes upon receiving only one accusation from a neighboring node. This scheme maintains two different lists warning list, and also black list in order to guard against malicious nodes. Moreover, by adopting the clustering architecture, the cluster head can address false accusation to revive the falsely revoked nodes.

The schemes that all nodes have already received certificates before joining the network each node are able to detect its neighboring attack nodes which are within one-hop away.

2.3 CLUSTER CONSTRUCTION

Nodes cooperates to form clusters and each cluster consist of a cluster head along with some cluster members located within the transmission range of their cluster head before nodes can join the network, they have to acquire a valid certificates from the certificate authority which is responsible for distributing and managing certificates of all nodes, so that the nodes can communicate with each other.

In this model, if a node proclaims itself as a cluster head, it propagates cluster head packet to notify neighboring nodes periodically. The nodes that are in this cluster head's transmission range can accept the packet to participate in this cluster as cluster members. When a node is deemed to be a cluster member, it has to wait for cluster head packet. Cluster head and cluster member keep in touch with each other.

Cluster member is assumed to belong to two different clusters in order to provide robustness against changes in topology. In case a cluster member moves out of the transmission range of its cluster head it has to search for other cluster head packet to participate in a new cluster.

Cluster means the nodes form the grouping. Each cluster has much number of nodes each node is have the node ID. Each node is moving in the cluster network so the nodes id changed with respect to mobility. The node allocation is represented by 0 and 1.

The nodes are present in the network is 1. The nodes are absent in the network is 0. The node id for a database is computed once, so even though that node actual IP address may change over time. Social network analysis is used to reduce the complexity of the node.

2.4 CERTIFICATE AUTHORITY FUNCTION

Certificate authority is deployed in the cluster based scheme to enable each mobile node to pre-load the certificate. The certificate authority is also update two lists, warning list, black list which are used to hold the accusing and accused node's information respectively.

The black list is responsible for holding the node accused as an attacker, while the warned list is used to hold the corresponding accusing node. The certificate authority updates each list according to received control packets. Certificate authority broadcasts the information of the warned list and black list to the entire network in order to revoke the certificates of nodes listed in the black list and isolate them from the network.

2.5 RELIABILITY BASED NODE CLASSSIFICATION

According to the behavior of nodes in the network, three types of nodes are classified according to their behaviors a legitimate node is deemed to secure communication with other nodes in a network. It is able to correctly detect an attack from malicious attacker nodes and accuse them positively and to revoke their certificate in order to guarantee network security. A malicious node does not execute protocols to identify misbehavior, vote honestly and revoke malicious attacker. Attacker node is defined as a special malicious node which can launch attacks on its neighbors to disrupt secure communication in the network. When a node joins the network and does not launch attacks it is regarded as a normal node with high reliability that has the ability to accuse other node. Normal node consists of legitimate node and potential malicious nodes. Nodes which are listed in the warning list are deemed as warned nodes with low reliability. Warning list contains a mixture of legitimate and few malicious nodes.

2.6 CERTIFICATE REVOCATION

To revoke a malicious attacker's certificate to consider three stages such as accusing, verifying, and notifying. The revocation procedure begins at detecting the presence of attacks from the attacker node. Then the neighboring node checks black list to match whether the attacker has been found or not. If not found the neighboring node casts the accusation packet to the certificate authority. The procedure of revocation

Step1: The neighboring nodes B,C,D and E detect attacks from node M

Step2: Each of them sends out an accusation packet to the certificate authority against M

Step3: According to the first received packet, the certificate authority hold B and M in the warned list and black list respectively after verifying the validity of node B

Step4: The certificate authority disseminates the revocation message to all nodes in the network

Step5: Nodes update their local warned list and black list to revoke M's certificate.

The false accusation of a malicious node against a legitimate node to the certificate authority, will degrade the accuracy and robustness to detect false accusation and restore the falsely node can be accomplished by its cluster head by its sending recovery packet.

Certificate authority disseminates the information of the warned list and black list to all the nodes in the network and nodes are update their black list and warned list from the certificate authority.

III. PERFORMANCE ANALYSIS

Under coalition list multi path transmission of a packet is considered.

Table.1 Comparison of Attackers

Coalition list	Optimum list	Revocation list
10	10	3
9	8	3
9	9	2
7	6	1
11	9	2

The optimum list founded by using voting mechanism with coalition listed nodes.

Table.2 Comparison of Encounters

Coalition list	Optimum list	Revocation list
6	6	4
8	7	5
7	7	4
6	6	1
7	6	2

By considering the probability of each node in a network the final list is formulated.

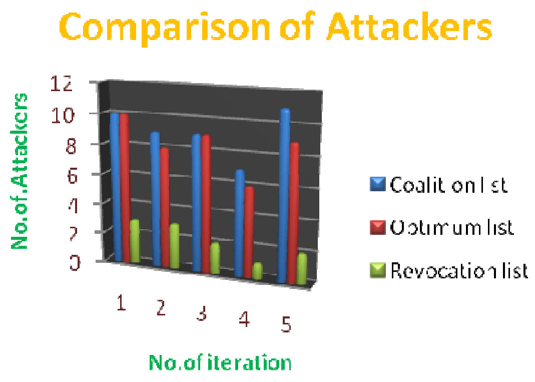

Fig.3 Comparison of Attackers

The Fig.3 shows the comparison of attackers. The attackers present in the coalition list minimized by considering number of votes gathered by attacker as well as the probability.

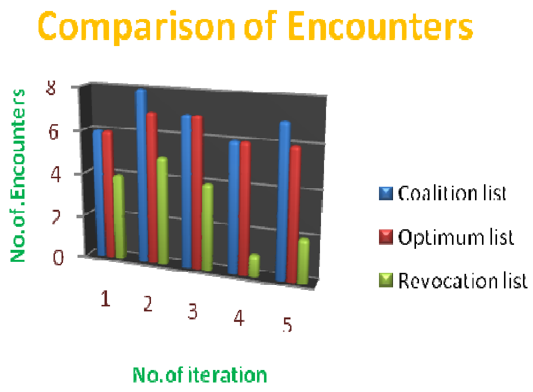

Fig.4 Comparison of Encounters

The comparison of encounters shown in the Fig.4.For encounters the probability is considered as an important factor.

IV. CONCLUSION

This research paper addresses the behavior of each node present in hybrid wireless networks which is more important in terms of the environment by forming the coalition structure with the help of voting mechanism. An effort has been made to concentrate on cooperative packet delivery without affecting the communications in the networks. For accurate certificate revocation the Cluster-based Certificate Revocation with Vindication Capability (CCRVC) was used. This method formed the stable coalition structure.

REFERENCES

[1] S. Pai, T. Roosta, S. Wicker, and S. Sastry, “Using Social NetworkTheory Towards Development of Wireless Ad Hoc Network Trust,” Proc. 21st Int’l Conf. Advanced Information Networking and Applications Workshops, pp. 443-450, May 2007

[2] S.C. Nelson, M. Bakht, and R. Kravets, “Encounter-Based Routingin DTNs,” Proc. IEEE INFOCOM, pp. 846-854, Apr. 2009.

[3] Q. Li, S. Zhu, and G. Cao, “Routing in Socially Selfish Delay Tolerant Networks,” Proc. IEEE INFOCOM, Mar. 2010.

[4] R. Lu, X. Lin, and X. Shen, “SPRING: A Social-Based Privacy-Preserving Packet Forwarding Protocol for Vehicular DelayTolerant Networks,” Proc. IEEE INFOCOM, pp. 1-9, May 2010.

[5] W. Gao and G. Cao, “On Exploiting Transient ContactPatterns for Data Forwarding in Delay Tolerant Networks,”Proc. IEEE 18th Int’l Conf. Network Protocols (ICNP), pp. 193-202, Oct. 2010.

[6] Khajonpong Akkarajitsakul, Ekram Hossain, Dusit Niyato, Member ,”Cooperative Packet Delivery in Hybrid Wireless Mobile Networks: A Coalitional Game Approach”, IEEE Transactions on Mobile Computing, vol. 12, no. 5, may 2013