Volume 3, Issue 5, May 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Secure Reputation-Based Clustering Algorithm for Cluster based energy optimized Mobile ad-hoc network

Keshav Kumar Tiwari
M.tech Student,
NITTTR Bhopal (India).

Sanjay Agrawal
Professor Dept. Of Computer Engineering Applications, NITTTR, Bhopal (India).

Abstract— An economical approach for organizing large ad hoc networks is to divide the nodes into multiple clusters and designate for every cluster, a cluster head that is accountable for holding inter cluster control information. In Clustering, ad-hoc networks are divided into groups which are managed by elected nodes known as cluster heads. It is an area co-ordinator of a cluster. It performs intra-cluster routing such as packet forwarding etc. A Cluster head performs the resource management function for its member nodes and perform inter-cluster and intra-cluster communication. This technique has been used for various goals as the efficiency of routing, transmission management and knowledge assortment. So much as we all know, no existing cluster algorithms have taken into consideration the existence of malicious nodes for cluster heads election and maintenance. In this paper, we tend to analyse the security drawback within the hierarchical mobile ad hoc networks. Then we propose a secure clustering algorithm supported based on reputation in defence of threats in clustering. In this algorithm, the nodes' reputation is used to improve security of cluster which is evaluated by combining the occurrence of the node in the routing process. In addition, we consider the degree and relative mobility within the cluster to ensure the stability of clusters. The weight of every node is computed through considering the on top of three factors at the same time. It's used to elect the secure backbone nodes within the networks. Moreover, it's economical within the cluster reconstruction and healing, and this proposed work is totally different than other research is working at the time now.

Keywords— MANET, Hierarchical Ad Hoc Networks, Clustering algorithms, Threat Security, Reputation based clustering algorithm (RECA).

I. INTRODUCTION

Clustering in MANET is defined as virtual partitioning of nodes into sub networks according to geographical area. Mobile ad hoc network (MANET) is the cooperative engagement of a collection of wireless mobile nodes without any predefined infrastructure relied on to keep the network connected. As ad-hoc networks don't have any fixed infrastructure, all network functions are performed by the mobile nodes themselves in a very self-organizing manner. This gives a lot of vulnerability in ad hoc networks, creating the problem of security problem and difficult [1]. In MANET a cluster design guarantees the basic performance accomplishment in a network with a large no. of mobile nodes. A cluster structure makes ad-hoc networks appears smaller and more stable. If a node changes its cluster then only nodes residing in corresponding clusters are ought to update the data no need the changes to be seen by the entire network. With the expansion of ad-hoc networks, the structure of hierarchical network has received so much attention because of its measurability in large-scale networks. According to the various types of objectives and needs, clustering schemes target completely different metrics, like the node's mobility, energy, connection and load balance.

Cluster head and gateway are the key nodes (i.e., Backbone nodes) in hierarchical ad-hoc networks. In MANETs a cluster-based communication infrastructure is employed for broadcasting. It additionally reduces collision in networking, energy consumption, and delay in packet transmission. It conjointly improves turnout of the network [2]. In cluster-based architectures, every cluster or cluster includes a cluster head that is accountable for traffic management. The cluster head possesses valuable info regarding nodes' location and their contacts. The lowest-ID cluster algorithmic program the highest-degree cluster algorithmic program and also the weighted bunch algorithmic program area unit the everyday bunch algorithms. Most clustering algorithms assume that the network setting is reliable and has no threats. In fact, ad hoc networks are simple to be wiretapped, intruded and attacked, due to the open distributed network structure. There are lots of attack interference measures, like encoding and authentication which will be used in a MANET to reduce intrusions, however not eliminate them. Therefore, we want to develop an efficient detection measure to the bone cluster structure for network security, like clustering in hierarchical ad-hoc networks.

In MANET any node can join the network, leave the network at point of time and can communicate with any other node; so authentication of communicating nodes before the transmission of actual data is a prerequisite. The proposed

authentication protocol needs to consume low computational power and minimum delay. In a MANET, secure communication protocol should satisfy the following security requirements. [3][4]

Confidentiality: Information of message is kept secure from unauthorized party. Confidentiality is sometimes called secrecy or privacy.
Data Integrity: Message is unchanged throughout the communication.
Authentication: Correct identity is thought to communicating partner.
Non-repudiation: Non repudiation ensures that the sender and receiver of a message cannot deny that they have ever sent or received such a message.

In this paper, we propose a reputation based clustering algorithm (RECA) .The nodes' reputation is used to enhance security that is evaluated by combining the experience of the node in the process of routing. Additionally, we consider a degree and relative mobility in the clustering to guarantee the stability of clusters

II. RELATED WORK

In order to produce security to MANET in past researchers has performed their research in software package as well as in hardware fields to form the mobile ad hoc network secure for use. MANET is in several fields to supply useful services. Zhang and Lee [5] proposed design based on distributed and cooperative nature of MANET nodes. Researchers have proposed a variety of cooperative IDS systems to address these challenges. In general, cooperative IDSs can perform better populated densely inhabited MANET with restricted mobility, and can perform worse in a sparsely populated MANET with significant mobility. Tomas Johansson and Lenka Carr-Motyˇckova [6] have proposed a clustering in ad hoc Networks. It makes it possible to define a limit for the maximum size of the clusters in addition because the maximum number of hops between a node and its cluster head. A local intrusion detection system (LIDS) with each node is extended for world concern to seek out the intrusion additional effectively. To create clusters, distributed algorithms are studied extensively [7,8]. Olivier Camp and Jean-Marc Percher [9] introduced the distribution of the intrusion detection mechanism by implementing a local Intrusion Detection System (LIDS) on every node. So as to form this detection a global concern for the community, the various LIDS coexisting within it, ought to collaborate. This would extend every LIDS's vision of the network. Jung-San Lee and Chin-Chen Chang [10] have projected a protocol using node identities to provide secure communication for cluster – based ad hoc networks. Their protocol is based on identity based scheme. It consists of two phases, like authentication and communication phase. It consists of trusted third party (TTP), that takes care of generating and issue the key information to every concerned node.

When a node needs to join the cluster it has to get the authentication token from the cluster head by executing the authentication part with the cluster head. TTP generates and distributes a secret key for every node and for each cluster head through a secure channel. CORE [12] proposed a watchdog for observation and isolating self-serving nodes supported a subjective, indirect and functional reputation. Confident [13] proposed using an adaptive Bayesian reputation and trust system wherever nodes monitor their neighbourhood and detect many varieties of wrongful conduct. SCAN [11] projected a network layer security protocol that depends on collaborative localised voting to convict malicious nodes and using uneven cryptography to protect the token of normal nodes.

III. ATTACKS IN CLUSTERING

Security of communication in MANET is very important for secure transmission of data. Absence of any central coordination mechanism and shared wireless medium makes MANET additional prone to digital/cyber attacks than wired network there are a variety of attacks that affect MANET. These attacks may be a cluster head, as defined in the literature, is a local organizer for its cluster, acting inter-cluster routing, information forwarding and then on. In our self-organized cluster scheme the cluster head only serves the aim of providing a unique ID for the cluster, limiting the cluster boundaries. According to the impact of the malicious nodes in the cluster, we tend to divide the attack into direct cluster attack and indirect cluster attack.

In the direct cluster attack, the malicious nodes discourage the cluster head election procedure, which is able to make the network difficult to make the clusters. Moreover, it's unable to establish the routing in clusters. Thus, this type of attack will more destroy the communication within the networks. Flooding [14] and rushing [15] are the typical direct clustering attack

To complete the indirect cluster attack successfully, first of all malicious nodes should be chosen as cluster heads with the advantage of fake metrics (e.g., degree and mobility) during the cluster head election procedure. After that, these malicious cluster heads will perform various attacks within the routing. Compared with the direct one, the indirect cluster attack is harder to be detected. Wormhole attack [16] is an example of this type attack. In the cluster, the attackers are successful to be the gateway nodes, and so they attack the network because the role of the backbone nodes.

In this Figure 1 shows the wormhole attack within the process of clustering. Node A and B are the malicious nodes in the wormhole attack, and that they are respectively in two wide separated clusters C and D. They associated with one another and send the cluster data to every other through the wormhole tunnel they build. And then, the malicious node will cheat the cluster head and be elected because the gateway node. That is, the wormhole attackers build a backbone link (C-A-B-D). They can do several types of attacks during this link, like black hole attack and resource consuming attack.

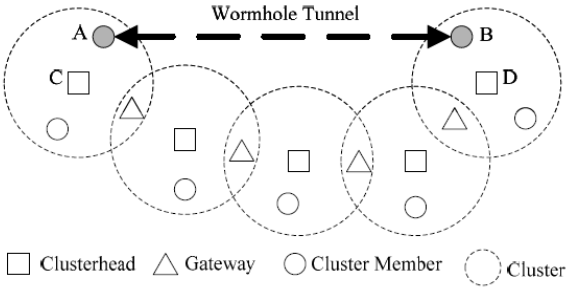

Fig 1: Wormhole attack in the process of clustering

IV. SECURE AND FAIR CLUSTER FORMATION

Cluster formation protocols verify a way to make group nodes and which of them are the most effective to be set up as cluster heads. Every protocol uses a particular utility function supported some metric (e.g. Node degree, remaining battery life, node mobility). The election of the suitable node to be a cluster head is threatened by two main vulnerabilities: (1) selfish attacks in which nodes cheat in order to not be elected cluster heads and keep energy and bandwidth for themselves, and (2) Greedy attacks in which nodes cheat to be elected cluster heads and have access to valuable data of the network topology and manages the traffic of the members of their cluster. To avoid them, the election of the cluster head should be fair (i.e. the elective node should be the one that maximizes the utility) and also the role must be rotative. The proposed algorithmic rule provides fairness and security to the cluster formation method using a distributed algorithm that monitors the system and checks if the information claimed by a node is coherent and reliable. We assume that maximum of network users is honest. So as to certify the information provided by every user and be able to track its behaviour, a mechanism supported symmetric ciphers, digital signatures and hash functions have been developed.

The cluster formation method consists of three sub protocols as follows:

1. The Cost Discovery Protocol provides reliable data concerning the measure used to measure the suitableness of a node to be a cluster head. This protocol uses a utility function based on the degree, i.e., the number of one hop neighbours. During this section, nodes publish the number of neighbours they have and exchange their specific perspective of the network to make a consensual view.
2. The Cluster head Designation Protocol selects the most effective suited node in a neighbourhood to be the cluster head supported some verifiable information provided by every node in the cost Discovery Protocol is correlative with data from different nodes.
3. The Cluster Management Protocol manages the cluster formation and realization once the cluster head is set up. Cluster nodes endorse the role of the elected cluster head by signing a claim. Then, the cluster head is ready up as a trusted authority for that cluster. The cluster head controls the licensed nodes that can work in its neighbourhood through the issuing of public key certificates that attest it.

V. REPUTATION EVALUATION IN CLUSTERING ALGORITM

Reputation based clustering algorithm (RECA) that aims to elect trustworthy, stable and high energy cluster heads that can be used to manage the security of the network. The reputation of the node is evaluated through the capability of the node in dealing with packets in the routing process. When we resolve node's reputation as a function of its centrality characteristics, we classify it as high, medium or low Centrality.

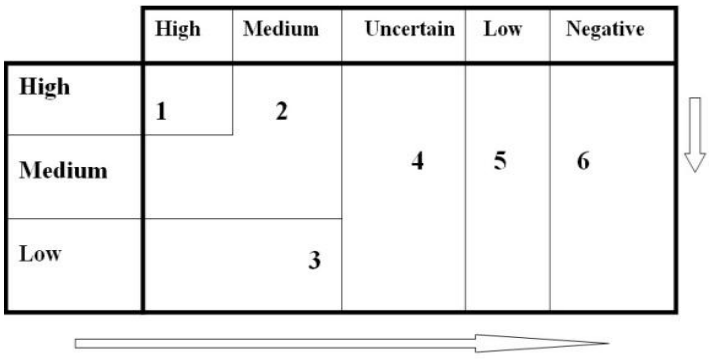

Figure 2: Self-Organized node selection for indirect-reputation information.

Fig. 2 shows how we classify the observed nodes into zones based on their reputation and centrality. Nodes falling into zone 1 are highly trusted nodes that also have a wider view of the network. Nodes that are classified as belonging to that zone have privileges such as higher watchdog expiration time and they are exempted from the deviation tests on their reported indirect reputation, low or no discounting factor, and high Reputation- Record expiration time. On

the other hand, nodes falling into zone 6 are known as miss-behaviour nodes, so their reported indirect-reputation is rejected. Nodes falling in zones between 1 and 6 would have different levels of acceptance and the different parameters would be adjusted to reflect their current zone. Nodes classification can change over time. This can be a result of a good reputation node that started to behave maliciously and hence become less trusted and fall to a less favourable zone. In ad hoc networks, the behaviour of the node involves the process of routing management messages and information packets in the routing. Attack measures of those two types of packets include forging, deleting, and tampering. Considering these, attack actions may be divided into selfish and malicious attacks. Therefore, we tend to classify the reputation of the node into selfish reputation (SR) and malicious reputation (MR) that denote the various aspects of nodes within the routing method. The reputation of the node is evaluated through the capability of the node in dealing with packets within the routing method.

The manifestation of a selfish attack is that the attacker drops the data packets in proportion, and its damage potential changes from quantity to quality, which might indicate the risk intensity through the accumulation of dropped packets. We assume that the activity of every node is random (i.e., the moving velocity of the node is uncertain.). Moreover, we measure the SR of every node by period and we assume that the numbers of positive and negative samples are S and F, respectively. The reputation value of selfish attack is written as-

$$R_f = \frac{S+1}{S+F+2} \qquad (1)$$

Compared with selfish attack, a malicious attack is fast, and if the condition the attack needs to operate is satisfied, it will destroy the network to a definite extent. Therefore, we set completely different values for the two types of reputation evaluation. In Selfish Reputation (SR) we set the value to 1. In Malicious Reputation (MR), the value will change with the degree of attack; that is the more serious the attack, the higher values are. The reputation value is calculated as follows.

$$R = \omega_f R_f + \omega_m R_m \quad (\omega_f + \omega_M = 1) \qquad (2)$$

VI. REPUTATION BASED CLUSTERING ALGORITHM (RECA)

In this paper, we proposed a reputation based clustering algorithm (RECA) that takes under consideration a combined weight metric, as well as the reputation value, the node's degree [17] and also the relative mobility [18]. The weight is calculated as follows:-

(1) Cluster head election- In the initial of creating a cluster, the nodes are assigned as the role (i.e., cluster head, gateway and cluster member) within the cluster through the clustering procedure. Every node broadcasts "Hello" message to its neighbour nodes periodically for connectivity.

After this, the weight information is carried in "Hello" message. When a node receives "Hello" messages from its neighbour nodes, it updates the reputation value of related nodes'. Additionally, the node will update its degree and mobility, according to the number of "Hello" messages received and the transmission power, respectively.

After receiving "Hello" message in some period of time, the node gets its initial weight. Then the node sends its weight through the broadcasted "Hello" message. Compared with different nodes' weight, the node that has the highest weight in the election of as cluster head is considered as CH.

If the node A receives the cluster head message from its neighbour node B, and node B's reputation value is more than A's, A can send the message to node B to join in its cluster. If node A has not received the cluster head's message throughout a period, it becomes an isolated cluster head that has no cluster member.

(2) *Cluster update*- Cluster update includes cluster reconstruct and cluster healing. Although the cluster is established, the topology of the network still might change because of the mobility of node, the falling of the energy and alternative factors. Thus, the node may leave the initial cluster, or the node may join in the cluster. The initial cluster will not be effective. This is cluster reestablishment. In the cluster filling procedure, we set the related value threshold according the node's role, i.e., TCH, TGW and TCM (TCH>TGW>TCM) are the thresholds of cluster head, gateway and cluster member, respectively.

When the node's reputation value is more than its role's reputation threshold, it's suspicious. And then, if this node is cluster head or gateway, search its neighbour's reputation value. If it is more than this suspicious node's, cancel the suspicious node's role of cluster head, and elect this node as cluster head. Else, keep the suspicious node's role. If the suspicious node is cluster member, place it into the blacklist and isolate from the network.

VII. CONCLUSION

In this paper we identify the threat security in hierarchic ad-hoc networks, and proposed a secure cluster algorithm based on reputation. In this proposed reputation framework which depends on the centrality and mobility as two key parameters to drive the system to a more stable state in highly mobile, distributed and disconnected environments. In this algorithm, a reputation evaluation mechanism based on the behaviours of nodes is built to achieve

accurate definition and precise quantization of reputation for nodes in the network. To improve the reliability of a cluster structure, this algorithmic rule considers the reputation, correlation and mobility of nodes in the method of electing cluster heads and gateways. Moreover, the reconstruction and the recovering mechanism in the algorithm are able to resist attacks on the cluster structure.

ACKNOWLEDGMENT

The Success of this research work would have been Uncertain without the help and guidance of a dedicated Group of people in our institute NITTTR Bhopal. I would like to express my special thanks of gratitude to my guide Dr. Sanjay Agrawal sir who gave me the golden opportunity to write this important paper on the topic "A Secure Reputation-Based Clustering Algorithm for Cluster based energy optimized Mobile ad-hoc network", which also helped me in doing a lot of Research and I came to know about so many new things, I am really thankful to them.

REFERENCES

[1] J. Luo, D. Ye, L. Xue, and M. Fan. A survey of multicast routing protocols for mobile Ad-Hoc networks. *IEEE Communications Surveys & Tutorials*, 2009, 11 (1): 78-91.

[2] X. Li, M.R. Lyu & J. Liu, "A trust model based routing protocol for secure ad hoc networks" in Proc., *IEEE aerospace conference* , vol. 2, pp. 1286–1295, March 2004.

[3] Hung-Yu Chien, Ru –Yu Lin Adhoc Networks, Improved ID based security framework for adhoc network, Vol.6, pp.47-60, 2007.

[4] HE Yijun, XU Nan and LI Jie A secure key exchange and mutual authentication protocols for wireless mobile communications, Proceedings of 2nd International conference on Availability, Reliability and Security, pp. 558-563, 2007.

[5] Zhang Y, Lee W. Intrusion detection in wireless ad hoc networks. Proc. Of 6th Ann. Int. Conf., (ACM MobiCom'00): Boston, MA, Aug 2000; 275-283.

[6] R. Draves, J. Padhye, and B. Zill, ―Comparison of routing metrics for static multi-hop wireless networks, sin Proc. of SIGCOMM '04, 2004.

[7] Vasudevan, Decleene B, Immerman N, et,al.Leader election algorithms for wireless ad hoc networks. In 3rd DARPA Information Survivability Conference and Exposition (DISCEX III): April 2003.

[8] Krishna P, Vaidya N H, et,al.A cluster-based approach for routing in dynamic networks. ACM SIGCOMM Computer Communication Review: 1997; 27, (2): 49-64.

[9] D. Johnson and D. Maltz (1996), ―Dynamic source routing in ad hoc wireless networks, ‖ in a book chapter in mobile computing, T. Imielinski and H. Korth, Eds. Dordrecht, the Netherlands: Kluwer, pp. 131-181

[10] Jung- San Lee and Chin-Chen Chang, Secure Communications for cluster – based ad hoc networks using node identities, Journal of Network and Computer Applications, Vol.30, pp.1377-1396, 2007.

[11] H. Yang, et al, "SCAN: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks," IEEE Network, vol. 24, 2006, pp. 1-13.

[12] P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks", Proc. IFIP CMS, 2002.

[13] S. Buchegger and J.L. Boudec, "A robust reputation system for peer-to-peer and mobile ad-hoc networks", proc. of P2PEcon, 2004.

[14] J. Kuo and W. Liao. Hop Count Distance in Flooding-Based Mobile Ad Hoc Networks with High Node Density. IEEE Transaction on Vehicular Technology. 2007, 56 (3): 1357-1365.

[15] G. Acs, L. Buttyan and I. Vajda. Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks. *IEEE* Transaction on Mobile Computing. 2006, 5 (11): 1533-1546.

[16] M. A. Azer, S. M. ElKAssas, A. W. F. Hassan and M.S. El-Soudani. Intrusion Detection for Wormhole Attacks in Ad hoc Networks a Survey and a Proposed Decentralized Scheme. *Availability, Reliability and Security*. 2008, pp. 636-641.

[17] E. M. Royer, P. M. Melliar-Smith, and L. E. Moser. An Analysis of the Optimum Node Density for Ad hoc Mobile Networks. *IEEE International Conference on Communications.* 2001, pp. 857-861.

[18] K. Xu, X. Hong and M. Gerla. An Ad Hoc Network with Mobile Backbones. *International Conference on Communications.* 2002, pp. 3138-3143.

