International Journal of Technology and Engineering System (IJTES)
Vol 7. No.1 2015 Pp. 54-58
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-1345

TRUST AND REPUTATION MANAGEMENT BASED CLUSTER HEAD SELECTION IN MOBILE AD-HOC NETWORKS

[1]SUJA RAJESWARI .K, [2]ARIVAZHAGI .A
Department of Computer Science and Engineering
[1]Valliammai Engineering College, [2]University college of Engineering- Ariyalur
Chennai, India
[1]ksrsuja@gmail.com,[2]arivupra@gmail.com

ABSTRACT

Mobile ad-hoc network is a infrastructure less communication network which does not rely on a pre-existing infrastructure. Security is the challenging task in MANET. Insecure wireless communication aggravates the vulnerability of ad-hoc networks. This paper is about the trust and reputation management and set to integrate the trust in a security framework in cluster head selection. This ensures the reliability, integrity, availability and trustworthiness of data sensed by the cluster node.

***Keywords:-*Clustering, Trust, Reputation management, Mobile ad-hoc network.**

I. INTRODUCTION

MANET is the infrastructure less multi-hop network which is characteristised by dynamic topology due to node mobility, speed,bandwidth and battery power of nodes. Moreover, an authority responsible for distribution of keys for the whole network is vulnerable to single point failure. So we require a distributed architecture for this kind of network for its proper functionality. Any node must be prepared to operate in a mode that should not immediately trust on any peer This paper address the problem of trust management based routing in mobile ad-hoc networks. To avoid the overhead of handling the network as a whole, nodes are grouped into clusters. In this paper we introduce a trust based approach for Cluster head (TA) selection algorithm [1]. Each cluster is nothing but a group of nodes which is headed by one or more node(s) known as Cluster head(s)(TAs).

In our proposal Cluster head is elected by the member nodes in order to make the TA more stable depending upon some metrics. This paper evaluate quantitative trust evaluation algorithm at each node to evaluate the direct trust of its neighbor nodes. The Node-based Trust Management (NTM) scheme is based on a Clustered mobile sensor network with backbone; it introduces a trust of a node within local management strategy with help from the mobile agents running on each node. That is, a node's trust-based information is stored as a history on the node itself.

Rest of the paper is organized as follows: Section 2 provides the summary of related work in trust and reputation management in ad-hoc networks. Section 3 discuss the threats. In Section 4,a trust management and reputation based clustering is proposed. In Section 5 discuss the results and followed by conclusion in Section 6.

II. RELATED WORK

A. Trust Concepts

The objective of trust based systems is to identify and isolate malicious nodes from the routing process. Trust is the measure of belief about the behavior of other entities (or nodes). Trust models compute the trust rating of a node with direct and/or indirect observations. The trust value of a node will be incremented by one unit for every positive experience and decremented by one unit for every negative experience.

The experience is in the view of executing the network activities such as the number of packet forwards, packet integrity maintaining and others. Apart from routing, the trust models are utilized in secure data aggregation, intrusion detection, secure localization, and others [2].

B. Greedy Perimeter Stateless Routing [3]

Among available GR protocols, Greedy Perimeter Stateless Routing (GPSR) is a baseline protocol, which

works with an extensive use of location information. GPSR works in two modes: Greedy mode and perimeter mode. In Greedy mode, an efficient path will be identified to reach destination. In perimeter mode, the routes are identified along the perimeter of the region. This mode is used when greedy mode fails to find a path towards the destination. In addition, for routing decisions, GPSR maintains information related to distance of the neighbors, link state of neighbors, and a path vector. All routing decisions are made with one hop information. The distance between neighbors is maintained through periodic beaconing location information. In mobile networks, a node may discover new nodes and its existing neighbors can dis-appear.

A fresh list of neighbors is maintained with periodic removal of dead nodes. A well known graph traversal rule called right hand traversal rule is employed in the protocol for perimeter forwarding of packets. During perimeter forwarding the graph planarization techniques are used to avoid crossing paths in the network. A node identifies the state of the other node with the promiscuous use of the network interface. Both greedy and perimeter methods provide full GPSR protocol. Perimeter mode operates on planar graph when the greedy mode on a full network graph fails.

C. Trusted GPSR (T-GPSR) [4]

Pirzada et al. [14] have utilized the trust concepts with GPSR (T-GPSR). T-GPSR considers two service criteria: the number of packet forwards (Pf) and the number of packet forwards without tampering (Pwt). A node X computes the trust rating of its neighboring node Y with these observations as

$$T(Y) = W(Pf) * Pf + W(Pwt) * Pwt \quad (1)$$

Where W(Pf) and W(Pwt) are the weights associated with each observation. These weights are set as 0.25 and 0.75 respectively.

D. Balanced Weighted Trust based GPSR (BT-GPSR) [5, 6]

Unlike conventional weight based models, the authors in [15, 16] have proposed a model (Balanced Weighted Trust base GPSR) that adjusts the weights associated with the observations of network activities. This model uses the ad-vantage of conventional weight based systems and Beta trust system [20] with adaptive weight adjustment to make efficient routing decisions. In addition, this model utilizes periodic observations, systematic trust computation and systematic trust application. In BT-GPSR, direct trust has been considered to restrict slandering attacks such as ballot stuffing and bad mouthing.

Ballot stuffing is an attack in which a malicious node promotes itself with high trust value. Whereas in bad mouthing attack, a malicious node intentionally damages other node's reputation by continuously advertising poor trust value. Due to the flexibility of weights adjustment, BT-GPSR dynamically identifies malicious nodes and directs the packets towards trustworthy nodes.

E. Reputation based secure GPSR (ATSR) [7]

Ambient Trust based Secure Routing (ATSR) [17] is a reputation based secure geographic routing method which combines the trust value computed from direct observations and reputation ratings obtained from neighboring nodes. ATSR considers 8 network activities for direct observation such as the number of packet forwards, network acknowledgement, packet precision, authentication, confidentiality, reputation responses, reputation validation, and remaining energy.

The direct trust expectation of the network activities is calculated as the ratio of number of successful transactions to the total number of transactions. Let A and B be the sensor nodes, the trust between A and B about a network activity m is calculated as

$$T_{A,B} = S_{A,B}/(S_{A,B} + F_{A,B}) \quad (2)$$

where $S_{A,B}$ is the number of successful transactions and $F_{A,B}$ are the number m of failure transactions.

III. THREATS

- Replay attack that adversary replays the previously transmitted messages. Spoofed data attack that adversary intercepts, alters data and transmits them to the destination.
- Wormhole attack: that an attacker receives packets at one point tunnels them and replays them into another point in the network. This tunnel between two colluding attacks is known as a wormhole.
- Black hole attack that attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it. Then it drops all packets that receive instead of forwarding them.
- Gray-hole attack which is a routing misbehaviour that leads to dropping of messages. This attack consists of two phases. Regarding first phase, attacker advertises as having a valid route to destination and in second phase, attacker drops received packets occasionally.
- Sinkhole attack that a compromised node tries to attract and drops data from all neighboring nodes.
- Denial of service attacks that are aimed to complete disruption of ad-hoc network.
- Selfish nodes which use network for their advantage and do not participate in operations to save energy[9].

IV. TRUST MANAGEMENT AND REPUTATION BASED CLUSTERING

A. Assumptions

All nodes communicate via a shared bi-directional channel and operate in promiscuous mode. In other words, after each forwarding the node can hear if the intermediate node has forwarded the message to the destination or not. All nodes are identical in their physical characteristics, that is, if a node A is within the transmission range of B then B is also within the transmission range of A. It is also assumed that all nodes are equipped with a residual energy detection device and some energy consumption model. Using the pair-wise key pre-distribution scheme, keys are distributed over the nodes of the network.

After election, a network key is generated by the CHs. Fig 1 illustrates any node wants to become a CH has to get access to the network key which is only sharable by the CHs. There are other keys also for secure communication, CH-group-key, the pair-wise secret key generated by pair of neighboring CHs to communicate to each other. Each mobile node maintains a Trust-Table of its one hop neighbors along with trusted pair-wise key for peer to peer communication without intervention of CH. Maximum allowable distance between any mobile node and CH will be one[8][10][11].

B. Cluster head selection algorithm by trust management

In this section we consider the selection of Cluster heads (TAs) in a MANET of n nodes such that every node in this network is within distance h hops of a TA, for a given TRUST-VALUE. Here, in our model, the Cluster lifetime denotes the time from the point a node is elected as Cluster head until the point a node changes its status to normal node. It should be noted that the Cluster lifetime is dependent on mobility issues; the Cluster lifetime in MANETs depends on link stability. Thus, a neighbor node is kept in the neighbor table and discarded if there is no further Clustering message received. Initially, the Interaction History (IH) for all nodes has been considered as null or ≥ 1.

Algorithm for cluster head selection

Step 1: A node (say M) wants to be CH, broadcasts "START-SELECTION" message with its mobility, Speed, battery power value to all its one hop neighbors.
Step 2: Getting this message each node within its broadcast range, calculates the global weight of that candidate node using a global function.

Gw= w1*TV+w2*MV+w3*BP+w4*SP

where w1, w2, w3,w4 are different weights such that (w1+w2+w3+w4=1)
Step 3: If Gw is greater than a predefined threshold, the node will vote for M by signing a Leader Certificate. Sends it to M(the node).
Step 4: After a certain time interval, the candidate node will count how many certificates it has already received.
Step 5: If this is greater than n/2 (where n is the number of neighbor nodes), it advertises itself as leader and broadcasts the leader message with the set of node-ids who has voted for it.
Step 6: If any node finds that its id is falsely included, it will generate a warning message to all its neighbors.
Step 7: After certain time say TCH, neighbor nodes will sign a TrustCert Leader, sends it to M.
Step 8: Thus M becomes a Leader and the elector nodes who has signed the certificate becomes its member.

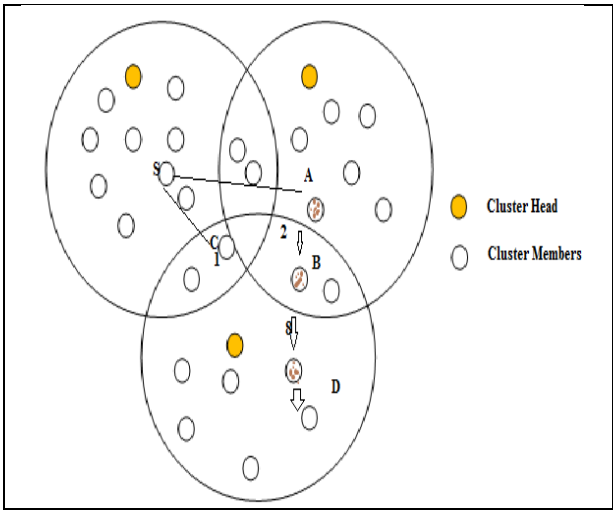

Fig 1. Clustering with CH

Trust-Value can be further evaluated by

$$\text{Tij } T(Y) = W(Pf) * Pf + W(Pwt) * Pwt \qquad (1)$$

Where W(Pf) and W(Pwt) are the weights associated with each observation. These weights are set as 0.25 and 0.75 respectively.

From fig 1.Due to the dynamic changes in the topology of network, the Cluster structure is updated from time to time[15]. It should be noted that whenever a node forwards a packet, it loses some amount of energy whose amount depends on factors such as the nature of packets, their size, access frequency, and the distance between the

nodes. Therefore we have assumed individual energy power in considering the path, that is, if there is a path with a node having very low energy level, then the available power function does not select that path, irrespective of whether or not that path is time efficient [12][13][14].The communication is based on the highest weight from node A to D. Source node send message by identifying highest weight of the nodes

C. REPUTATION BASED

The direct trust expectation of the network activities is calculated as the ratio of number of successful transactions to the total number of transactions. Let A and B be the sensor nodes, the trust between A and B about a network activity m is calculated as

$$T_{A,B} = S_{A,B}/(S_{A,B} + F_{A,B}) \quad (2)$$

where SA,B is the number of successful transactions and FA,B are the number m of failure transactions. This provides the trusted value and reputation value after clustering .The nodes which are less than 1 is considered as malicious node.

V. RESULTS AND DISCUSSION

The proposed trust based clustering framework along with a leader selection mechanism ensures that the cluster head selection and cluster formation in the ad hoc network is secure. It is to be noted that initially a node given the status suspicious node should be restricted to intra cluster communication until it gets Trust Certificate CERT. This certificate is also subject to review. As the trust value of a particular node depends on its participation towards proper functionality of the network each node must cooperate and the network can be prevented from inside malicious attacks.

Moreover, we use mathematical model and combine different opinion collected from different member nodes,this will provide the most probable belief and the prediction will be more accurate. It will help the cluster head to give the status of a member node and an overall trusted environment framework will be created.

VI. CONCLUSION

In this paper, we have proposed a new approach based on trust and reputation management for self-organizing clustering algorithm. Only few works have been done in this field. The majority of security solutions were based on cryptography which may not be well-suited with dynamic topology nature of ad hoc networks. We have used the trust evaluation mechanism depending on the behavior of a node towards proper functionality of the network. Our trust evaluation model gives a secure solution as well as stimulates the cooperation between the nodes of the network. We are not only restricting to direct observation for predicting trust but also recommendation from one hop neighbors of any node under review. The originality of our work consists of combining different trust mechanism for quantifying trust and the leader selection algorithm in order to predict the trust of mobile node more accurately based on cluster head and cluster member communication.

REFERENCES

[1] *R. Ferdous, V. Muthukkumarasamy and E. Sithirasenan, "Trust-based Cluster head Selection Algorithm for Mobile Ad hoc Networks", International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11, pp. 589-596,2011.*

[2] *Raghu Vamsi and Krishna Kant. Systematic design of trust man-agement systems for wireless sensor networks: A review. In Fourth International Conference on Advanced Computing & Communication Technologies (ACCT), pages 208–215. IEEE, 2014.*

[3] *Brad Karp and Hsiang-Tsung Kung. Gpsr: Greedy perimeter stateless routing for wireless networks. In Proceedings of the 6th annual international conference on Mobile computing and networking, pages 243–254. ACM, 2000.*

[4] *Asad Amir Pirzada and Chris McDonald. Trusted greedy perimeter stateless routing. In 15th IEEE International Conference on Networks ICON 2007, pages 206–211. IEEE, 2007.*

[5] *P. Raghu Vamsi, Payal Khurana Batra, and Krishna Kant. Bt-gpsr: An integrated trust model for secure geographic routing in wireless sensor networks. In 2014 Students Conference on Engineering and Systems (SCES), pages 1–6. IEEE, 2014.*

[6] *P. Raghu Vamsi and Krishna Kant. Adaptive trust model for secure geographic routing in wireless sensor networks. In 2014 Seventh International Conference on Contemporary Computing (IC3), pages 394–399. IEEE, 2014.*

[7] *Theodore Zahariadis, Panagiotis Trakadas, Helen C Leligou, Sotiris Maniatis, and Panagiotis Karkazis. A novel trust-aware geographical routing scheme for wireless sensor networks. Wireless personal com-munications, 69(2):805–826, 2013.*

[8] *R. Agarwal and M. Motwani, "Survey of clustering algorithms for MANET", International Journal on Computer Science and Engineering, vol. 1, no. 2, pp. 98-104,2007.*

[9] *P. Goyal, S. Batra and A. Singh, "A Literature Review of Security Attack in Mobile Ad-hoc Networks", International Journal of Computer Applications, vol. 9, pp. 11-15, November 2010.*

[10] *S. Peng, W. Jia and G. Wang, "Voting-Based Clustering Algorithm with Subjective Trust and Stability in Mobile Ad-Hoc Networks", IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, pp. 3-9,2008.*

[11] *B. Kadari, A. Mhamed and M. Feham, "Secured Clustering Algorithm for Mobile Ad Hoc Networks", IJCSNS International Journal of Computer Science and Network Security, vol. 7, no. 3, pp. 27-34, ,March 2007.*

[12] L. Wang and F. Gao, "A Secure Clustering Scheme Protocol for MANET", International Conference on Multimedia Information Networking and Security (MINES), pp. 785-789,2010.

[13] P. Chatterjee, "Trust Based Clustering And secure routing Scheme for Mobile Ad Hoc Networks", International Journal of Computer Networks & Communications, vol. 1, no. 2, pp. 84-97, July,2009.

[14] Y. Yu and L. Zhang, "A Secure Clustering Algorithm in Mobile Ad Hoc Networks", IPCSIT, vol. 29, 2012.

[15] V. Palanisamy and P. Annadurai, "Trust-based clustering for multicast key distribution scheme in ad hoc network (TBCMKDS)", Journal International Journal of Internet Protocol Technology, vol. 6, no. 1-2, June 2011.