Asian Journal of Information Technology 15 (23): 4806-4811, 2016
ISSN: 1682-3915

Stable Clustered Topology and Secured Routing Using Mobile Agents in Mobile Ad Hoc Networks

K. Sangeetha, P. Vishnuraja and D. Deepa
Department of Computer Science and Engineering, Kongu Engineering College,
638052 Perundurai, Tamil Nadu, India

Abstract: Mobile Ad hoc Networks (MANETs) are dynamically vibrant network with the vital issues to be addressed as routing and security. For competent functioning of the network it is essential to establish a secured and topologically stable network. This is achieved by constructing a stable clustered topology based on residual energy calculation and by detecting the malicious nodes using mobile agents. Based on the nodes energy, rank is calculated for each node and the cluster head is chosen by the mobile agents. The mobile agents are checking whether a node is trustable one to participate in the network. Credit system is introduced to increase the trust of the nodes.

Key words: Clustering, topology, QoS, security, mobile agents

INTRODUCTION

MANETs are susceptible to variety of attacks that embody passive eavesdropping, denial-of-service, impersonation and active interfering even though, intrusion interference measures like robust authentication redundant transmission can be accustomed to improve the protection of those networks. These techniques will address solely a set of threats and that they are very expensive to implement. The dynamic nature of circumstantial networks needs interference techniques that ought to be complemented by detection techniques to observe security of the network and determine any malicious behavior. Intrusion detection is a second line of defense that has native security to a node and additionally helps in establishing a particular trust level of a node in an ad-hoc network. Since, it is not possible to adopt a totally centralized approach to security in circumstantial networks, a cluster-based distributed approach is adopted that helps in integration of native intrusion detection during a cluster with network wide global intrusion detection (Gomez and Campbell, 2007; El-Defrawy and Tsudik, 2011; Saha *et al*., 2007).

In the proposed research work, MANET is divided into different clusters using a stable clustering algorithm. The clustering makes the communication between the nodes in the network more efficient as each cluster is managed by its cluster-head and inter-cluster communication takes place only through the gateway node. The task of cluster management in a cluster is delegated to the cluster-head which is chosen based on the output of an algorithm that is invoked periodically. The rotation of cluster management responsibility to different nodes ensures a correct load leveling and fault-tolerance within the system. It is proposed to delegate the cluster-wide intrusion detection responsibility to the mobile agents, apart from their default function of cluster management. They can initiate a cooperative approach for intrusion detection. The different mobile agents in the network maintain a database of known attacks.

MATERIALS AND METHODS

The Stable Clustered Topology and Secured Routing (SCTSR) algorithm is based on the introduction of mobile agents and supervisory mobile agents for improving the performance of the network. The mobile agents are applying the logic to determine the nodes probability to become a cluster head. The nodes in the network form the cluster and the node information like node ID, energy level, transmission range are sent through Hello messages and the node with maximum energy level is chosen as the cluster head. Based on the information received from different hello messages of the nodes, the node with the highest residual energy level is determined by the mobile agents. This node becomes the cluster head. In the stable cluster algorithm concept the responsibility of the cluster head is reduced by introducing the mobile agents for verifying the selection of the cluster head, maintaining the

Corresponding Author: K. Sangeetha, Department of Computer Science and Engineering, Kongu Engineering College, 638052 Perundurai, Tamil Nadu, India

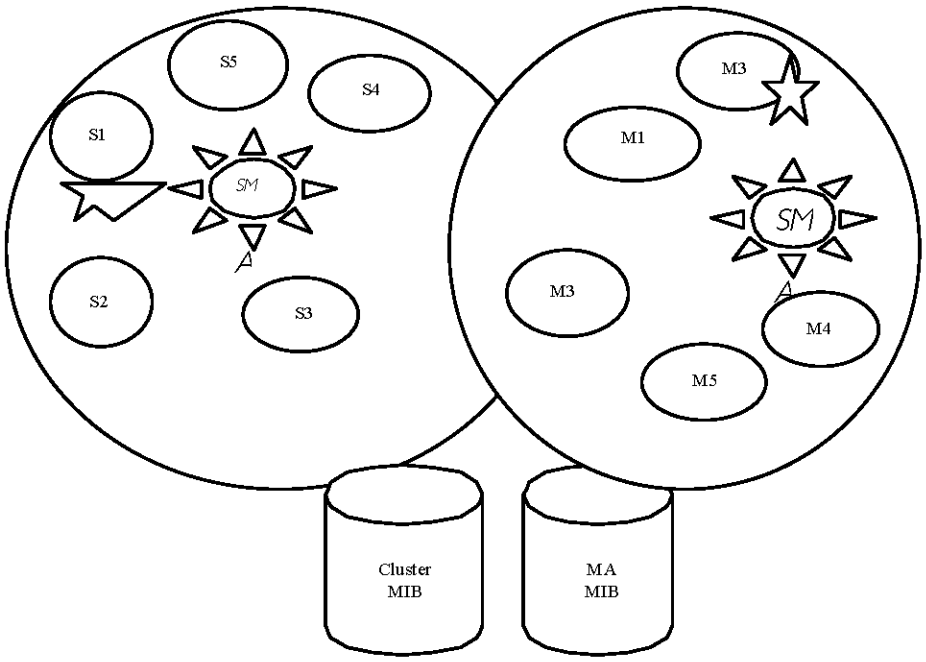

Fig. 1: Architecture of the secure clustered MANET

Table 1: Structure of C-MIB

Cluster ID	Current cluster head	Residual energy leve l (J)	Selfish node	Malicious node	Pure list
C1	S1	450	-	S3	S2,S4,S5
C2	M2	340	M4	-	M1,M2, M3,M5

Table 2: Structure of MA_MIB

ClusterID	Current MA No.	MA backup time (ms)
C1	MA1	1.5
C2	MA2	4.3

cluster head and securing the cluster from the malicious nodes locally. The supervisory mobile agent is introduced to verify the Mobile Agent Management Information Base (MA-MIB), secure the mobile agents and backup the mobile agents and in turn initiates the global intrusion detection system (Chauhan *et al*., 2011; Hanzo and Tafazolli, 2011; Gomez and Campbell, 2007).

The mobile agents are created to detect a stable cluster and to eliminate the malicious nodes in the cluster network. After a time t, the mobile agents are created and they move to the nearby nodes and its first and foremost function is to verify the energy level of each node. The selfish behavior of the nodes is detected. It initiates local intrusion detection within the cluster. All the details of the mobile agent are stored in the MA-MIB as in Fig. 1.

Formation of cluster: The Mobile Agent Management (MAM) algorithm is deployed in the formation of the clusters. When the nodes are passing the hello messages, the MAM algorithm creates the Supervisory Mobile Agent (SMA) and Mobile Agent (MA). As soon as the agents are generated from the algorithm both the agents start performing various functions. The MA creates the Cluster Management Information Base (C-MIB) in which the following details are added as in Table 1 at a particular time t.

The other functionalities of MA are verification of cluster head. It initiates local intrusion detection algorithm which helps in detecting selfish and malicious nodes. Simultaneously the SMA creates Mobile agent Management Information Base(MA-MIB) in which the following details are stored as in Table 2.

The other functionalities of SMA are verifying the MA-MIB, initiating the backup of MA, initiating global intrusion detection algorithm which help in detecting the risks and the severity of the risks. The actions are taken and informed to the source nodes about the risks. Earlier it had been the responsibility of a cluster-head to inform the neighboring cluster-heads about any network-wide intrusion response action which is further propagated to the cluster members of the neighboring clusters. But now it has been taken over by the SMA.

Election of cluster head: The MA takes the charge to calculate the clustering coefficient of the nodes and rank of the nodes. The clustering coefficient of node for

Table 3: Structure of PDR details

Source ID	Destination ID	Threshold PDR	Hop count
S1	M1	40	3
S1	M2	26	4

instance A is the ratio between the actual number of links between the neighbors of node A and the maximum possible number of links between these neighbors. Also, the clustering coefficient is the ratio between the number of triangles that may contain the node A and the number of triangles that would contain A if all neighbors of A are interlinked. The cluster radius specifies the range of the cluster and it gives how far the farthest node inside a cluster can be from the cluster head. The nodes which do not need relaying when node Atransmits to them are called neighbors of node A (Rekik *et al*., 2011).

The rank is locally calculated for each node based on the power which is used for cluster head election using Eq. 1. The rank is calculated based on the initial energy Ei residual energy Er, cluster radius, r distance of the node A from the neighboring node B, d:

$$R = (r - \frac{d}{6r} \times (\frac{E_r}{E_i}) \quad (1)$$

The cluster head will consume much more energy than the rest of the nodes since it needs to forward all data from the nodes inside its cluster to the gateway nodes. If the nodes inside the cluster are more it leads to more consumption of energy. Based on the rank values the mobile agents make the decisions to elect the cluster heads. Based on the inference rules for the electing a node with maximum rank value the cluster head is elected. Each cluster is multi-level. There is no optimal number of levels. As no assumptions are about the size and topology of the network the number of levels in a cluster depends on the cluster range and the minimum energy path to the cluster head.

The clusters are generated before the communication is begun. The time to generate the cluster is Tg. Two types of communication can take place in a clustered network as intra-cluster and inter-cluster communication. The time for these two communications is Tc. To guarantee a good performance Tc should be Tg. To avoid a cluster head from drying out the mobile agent runs periodically every Tc+Tg. During Tg, each node runs same clustering algorithm to generate the clusters.

Maintenance of cluster head: The mobile agent periodically checks for the residual energy of each node which is updated in the C-MIB. Based on that the cluster head is re-elected and the rest of the nodes are intimated about the change of the cluster head (Ahmed *et al*., 2012; Liu *et al*., 2007).

When a new node enters the range of the cluster head it is properly authenticated by the supervisory mobile agent. The member registration algorithm of the global intrusion detection algorithm checks for the authentication of the node. The node which succeeds in this process is provided with a cluster Id. This is intimated to the cluster head and other members of the cluster by New-Member message. The new nodes ID and residual energy are obtained by the SMA during the authentication phase itself. Theseinformation are passed to the MA through the Update C_MIB command from the SMA.

There are possibilities that the energy level of the newly arrived node may be totally greater than the current cluster head. But it will not be elected as cluster head immediately. During the next phase of cluster election only the newly arrived node will be considered for cluster head election.

Detection of selfish nodes: The routing path is made highly secure using the mobile agents for detecting the malicious nodes. The nodes may behave selfishly and drop some packets which have to be forwarded to some other nodes. The reason for this selfish attitude is to save energy for their purpose. Those nodes may wish to transfer the packets from them to other nodes for which they have to reserve energy.

When a node initiates packet transfer from it to some other destination it will be sending the routing request which in turn will be received by MA. The MA now takes the responsibility to calculate the Packet Delivery Ratio (PDR) of all the nodes that are involved in the transmission of the packet. Table 3 is maintained by the MA for finding out the malicious node.

The source sends the RReq to MA from which the details of the source ID and Destination ID are determined .The routing is generated by simple AODV protocol and the number of hops is determined and stored in the structure. The Threshold PDR is calculated as given in Eq. 2 by taking the difference of the number of packets send from source, S_{pkt} and the product of the number of nodes in the cluster, N and 2:

$$Threshold_{PDR} = S_{pkt} - N \times 2 \quad (2)$$

Considering the Eq. 2 for transmission of packets from S1 to M1, the number of hops is 3 S1-S5-S4-M1 as analyzed from Fig. 2. If total number of packets to be sent from S1 to M1 is 50, then the $Threshold_{PDR}$ can be given as 50-5×2 which is 40. As soon as these details are updated

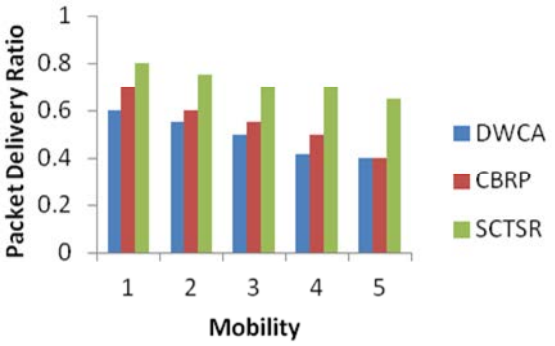

Fig. 2: Packet delivery ratio vs mobility (nodes-20)

Table 4: Structure of credits details

Node ID	Credits gained by forwarding packets (C_{gain})	Credits paid for sending packets (C_{paid})	Total credits
ID_N1	4	2	2
ID_N2	10	4	6

in the selfish node detection structure, the MA moves to the first node which is at the first hop to source in the routing path. It acquires the details of how many packets have been received by the node from the source, P_{rcd} and how many number of packets have been forwarded, P_{fwd} by the same node to the next hop node. The ratio of these two values gives the actual packet delivery ratio of the node as given in Eq. 3:

$$\text{Packet Delivery Ratio (PDR)} = \frac{P_{rcd}}{P_{fwd}} \quad (3)$$

The MA then compares it with the Threshold_{PDR} of that routing path with the current PDR calculated for the first hop node, node-PDR. When node-PDR of the node is greater than the threshold-PDR the node is marked malicious and a message is sent to the source. The source may now take decisions to remove the node from the routing path. This process is repeated continuously for all the nodes in the routing path from the source to the destination. The nodes ID would be mentioned under the malicious nodes list of C-MIB. The pseudo code of selfish node detection algorithm can be given as:

Algorithim:

If S wants to send n packets
to D through N nodes,
then Trigger Generation of
MA

MA
$\text{CalculatesThreshold}_{PDR}$
MA receives the node_PDR for each node involved in routing
MA compares with Threshold_{PDR} and node_PDR
If N_{PDR}>Threshold_PDR
then intimate N as malicious to S
S sends malicious node identity message to CH
CH marks N as malicious and adds to C_MIB
End If
End If

Selfish node correction: The nodes in the network are identified as selfish nodes by the mobile agents as they refer to the C-MIB. The Mobile agents take the turn to motivate the selfish nodes from participating in the packet forwarding by the Motivation Algorithm. The MA starts sending motivate messages to selfish nodes in the cluster informing about the credits. The selfish nodes are informed that the node would be getting credit values added to their account which would be beneficial to them as they forward the packets to other nodes. After passing these messages continuously for three times the nodes are unmarked from the selfish node list. The other nodes are intimated to forward packets via the unmarked node. The node-PDR is again noted for the unmarked nodes when they transmit the packets. If it is equal to the threshold value then the nodes are given the credits. The accounting of the credits gained by the nodes is maintained by the SMA as in Table 4.

$$\text{Total Credits} = C_{gain} - Cp_{aid} \quad (4)$$

The SMA provides services to the nodes only when the total credit as calculated in Eq. 4 is a positive integer. The SMA also insists that the total credits should always be optimally 20-50 according to which the nodes would get good or poor service from the MA/SMA. The pseudo code of motivation algorithm can be given as

Algorithim:

MA reads the selfish nodes from C-MIB
MA sends the Motivate Message to all
Selfish nodes
If message send >3,
Then unmark nodes as selfish
from C_MIB
Unmarked message given to CH
CH intimates all nodes
End if
If packet send by selfish node
Then credit = credit -1
Else if packet forwarded by selfish node
Then credit = credit +1
End if
End if

Securing the mobile agent: The functionality of MA is verified by the SMA periodically. The SMA verifies how often the C-MIB is updated as the simulation time proceeds. If the updating has been done long back with the time difference of > 5m sec then SMA ensures that MA is not working properly and initiates MA to back up the data. MA is not responding or its complete back up is

Table 5: Mobile agent RTT

No. of nodes	Round-trip time (m sec)
10	50.130
20	120.65
30	210.34

over, SMA deletes the MA. It initiates the creation of new MA and intimates this information to the CH, so that CH can take the responsibility of the network till the new MA is created.

Security analysis: The security analysis is carried out to determine the performance of the mobile agents by setting the numbers of mobile agents and selfish nodes in the network. The average size of a tracing agent is 4.2K bytes that of information-gathering agents without information are 2.1K bytes and 2.4K bytes with information. The measurement of the time period from when a node triggers to start agent generation and turns to the manager in each case of the number of target systems contained in an intrusion route is carried. It is done in the case of authenticating agents (Table 5).

RESULTS AND DISCUSSION

The research work is done using the NS2 simulator. The experiments are conducted in MANET scenarios in a topology of 1000×1000 m area. The total simulation time is set to 1000 sec and the bandwidth is set to 2 Mbps. Constant Bit Rate (CBR) traffic is used to send 512 byte packets between nodes. The queuing capacity of every node is set to 100. A random traffic generator in the simulation is adopted that chose random pairs of nodes and sent packets between them.

The initial locations are obtained using the Random Way Point (RWP) model of NS2.The mobility of the nodes vary from 0-10 m sec^{-1}. The variable range transmission is adopted for the mobile nodes. The simulation is carried for different levels of malicious nodes (denial of service) introduced into the network. The routing protocol used is the simple extended AODV implemented in NS2.The results are compared with standard clustered protocols like Cluster Based Routing Protocol (CBRP) and Distributed Weighted clustering Algorithm (DWCA).

In order to evaluate the effectiveness of the security framework, the simulation process is divided into two stages and compared the network performance in terms of three metrics. The malicious nodes are introduced into the MANET scenario after t secs and they vary from 10-50% that of normal nodes.

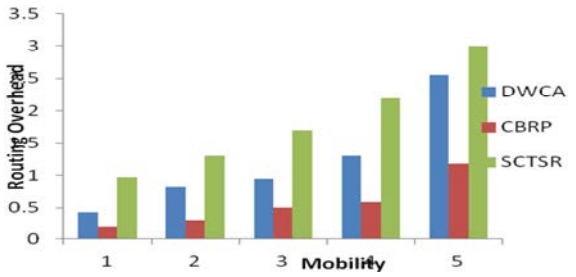

Fig. 3: Routing overhe

Packet delivery ratio: Under the normal situation the SCTSR and CBRP are performing same and the CBRP is performing poor than former as there are no energy management or cluster security measures. After the algorithms for stable clustered MANET are enabled the SCTSR is out performing the CBRP and DWCA in packet delivery ratio.

When the mobility of the nodes is increased the PDR is reducing but when compared to other algorithms it is highly improved as in Fig. 2. Similarly the increase in number of nodes is also well managed by the stable cluster algorithms.

Routing overhead: The Routing overhead is the one of the metrics which depends on the number of some stale routes are generated in the routing table as nodes often change their location within network. When the mobility of the nodes increases the overhead associated with routing also increases as in Fig. 3. Also the overhead increases drastically due to increase in the number of nodes.

End to end delay: The end to end delay is calculating the time elapsed between the source and destination nodes in the network. In the CBRP and DWCA approaches only the clustering is implemented to manage the network. When malicious nodes are introduced into the network, there is no way to detect them. So the end to end delay is more when compared to the SCTSR approach. When the number of nodes is varied the end to end delay is not affected as in the case of earlier clustered algorithm, CBRP or DWCA. This is because of the implementation of mobile agents in SCTSR.

When the mobility of the nodes is varied then the delay is depicted as in Fig. 4. In the research work the intrusion detection system with Mobile Agents (MA) for detecting the selfishness of the nodes is implemented. This helps in the utilization of resources effectively. The

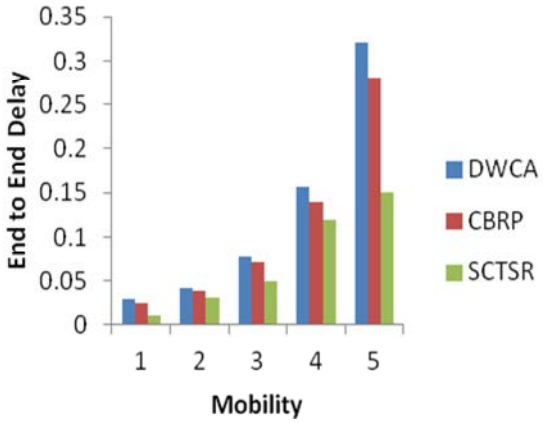

Fig. 4: End to end delay vs. mobility (nodes-20)

nodes with optimum energy may not be repeatedly elected as cluster leaders and only the nodes with high residual energy would be elected as cluster head. The malicious nodes are also detected from the IDS with the help of the Supervisory Mobile Agents (SMA). The SMA also helps in removing the corrupt MA code when the response time of MA exceeds or when the MA is not reachable. Backup of the Cluster-MIB is taken periodically and verified. When compared with the cluster based approach for managing the cluster the introduction of the mobile agents improves the security of the clustered MANET. The routing overhead encountered is compromised for adopting a secured MANET architecture.

CONCLUSION

Parameters considered for analysis are routing overhead, end to end delay and packet delivery ratio. Based on the simulation results the mobile agents are able to detect the malicious nodes within the mobile ad hoc networks.

REFERENCES

Ahmed, A., F. Khan, K.G. Rahatullah and Y. Ali, 2012. The role of mobile ad-hoc networking for pervasive computing. Int. J. Multi Disciplinary Sci. Eng., 3: 19-24.

Chauhan, N., L.K. Awasthi, N. Chand and A. Chugh, 2011. A Distributed Weighted Cluster Based Routing Protocol for MANETs. In: Computer Networks and Information Technologies. Vinu V.D., S. Janahanlal and C. Yogesh (Eds.). Springer Berlin Heidelberg, Berlin, Germany, pp: 147-151.

El-Defrawy, K. and G. Tsudik, 2011. ALARM: Anonymous location-aided routing in suspicious MANETs. IEEE Trans. Mobile Comput., 10: 1345-1358.

Gomez, J. and A.T. Campbell, 2007. Variable-range transmission power control in wireless ad hoc networks. IEEE Trans. Mobile Comput., 6: 87-99.

Hanzo, L. and R. Tafazolli, 2011. QoS-aware routing and admission control in shadow-fading environments for multirate MANETs. Mob. Comput. IEEE. Trans., 10: 622-637. Kuppusamy, S. and N. Mathaiyan, 2013. Intellisense cluster management and energy efficient routing in mobile ad hoc networks. J. Comput. Sci., 9: 1092-1098.

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: 536-550.

Rekik, J.D., L. Baccouche and H.B. Ghezala, 2011. Load-balancing and energy aware routing protocol for real-time flows in mobile ad-hoc networks. Proceedings of the 2011 7th International Conference on Wireless Communications and Mobile Computing, July 4-8, 2011, IEEE, Istanbul, Turkey, ISBN: 978-1-4244-9539-9, pp: 343-348.

Saha, A.K., K.A. To, S. PalChaudhuri, S. Du and D.B. Johnson, 2007. Design and performance of PRAN: A system for physical implementation of ad hoc network routing protocols. IEEE. Transac. Mob. Comput., 6: 463-479.