International Journal of Soft Computing 7 (6): 294-301, 2012
ISSN: 1816-9503
© Medwell Journals, 2012

Cluster Based Trust Mechanism for Mitigation of Internal Attacks in Mobile Ad Hoc Networks

[1]R. Murugan and [2]A. Shanmugam
[1]Department of Computer Applications,
[2]Department of Electronics and Communication Engineering,
Bannari Amman Institute of Technology, Sathyamangalam, 638401 Tamil Nadu, India

Abstract: The wireless nature and inherent features of mobile ad hoc networks make them vulnerable to a wide variety of attacks. In an internal attack, the attacker gains normal access to the network and takes part in the network activities. The major challenges related to securing ad hoc networks are to make ad hoc network unconditionally secure against different external and internal attacks security solutions should be energy efficient to perform the functionality of the network (routing the packets properly and securely) if some of the nodes are captured or any node goes out of the radio range. To avoid the overhead of handling the network as a whole, the nodes are grouped into clusters. The challenges can be handled by formalizing the trust relationship between the nodes. To enhance security, it is important to evaluate the trustworthiness of nodes without depending on central authority. In this study, a cluster based trust mechanism is evaluated to mitigate the internal attacks. The entire network is divided into hierarchical group of clusters. Each cluster having a fully trusted Cluster Head (CH). Each node calculates the trust value for its one hop neighbours and sends it to CH. In turn, the CH issues the trust certificate to its member nodes if the trust value is positive otherwise that particular node is declared as misbehaving node. By simulation results it is shown that the cluster based trust mechanism provides better packet delivery ratio and resilience against internal attacks.

Key words: Cluster, positive, resiliences, internal attacks, node

INTRODUCTION

A Mobile Ad Hoc Network (MANET) is a collection of dynamic, independent, wireless devices that groups a communications network, devoid of any backing of a permanent infrastructure. The eventual goal of designing a MANET network is to make available a self-protecting, dynamic, self-forming and self-healing network for the dynamic and non-predictive topological network (Orwat *et al*., 2008). According to the positions and transmission range, every node in MANET acts as a router and tends to move arbitrary and dynamically connected to form network. The topology of the ad hoc network is mainly interdependent on two factors; the transmission power of the nodes and the mobile node location which are never fixed along the time period (Saad and Zukarnain, 2009).

Ad hoc networks excel from the traditional networks in many factors like easy and swift installation and trouble-free reconfiguration which transform them into circumstances where deployment of a network infrastructure is too expensive or too susceptible (Huang *et al*., 2007). MANETs have applicability in several areas like in military applications where cadets relaying important data of situational awareness on the battleground, in corporate houses where employees or associates sharing information inside the company premises or in a meeting hall; attendees using wireless gadgets participating in an interactive conference, critical mission programmer for relief matters in any disaster events like large scale mishaps like war or terrorist attacks, natural disasters and all. They are also been used up in private area and home networking, location-based services, sensor networks and many more adds up as services based on MANET (Wu *et al*., 2006). The three major drawback related to the quality of service in MANET are bandwidth limitations, vibrant and non-predictive topology and the limited processing and minimum storage of mobile nodes (Uma and Padmavathi, 2009).

MANET attacks and classification: The wireless nature and inherent features of mobile ad hoc networks make them vulnerable to a wide variety of attacks. The attacks

Corresponding Author: R. Murugan, Department of Computer Applications, Bannari Amman Institute of Technology, Sathyamangalam, 638401 Tamil Nadu, India

on MANETs can be classified into various criteria as shown below (Shanthi *et al*., 2009; Xiao *et al*., 2007; Razak *et al*., 2004).

Passive attacks and active attacks: These attacks depends on whether the normal operation of the network is disrupted or not.

Passive attack: A passive attack intrudes the data exchange with in the network without varying it. Here, the prerequisite for privacy gets desecrated. Detection of passive attack is hard to detect as the operation of the network itself doesn't get affected.

Active attacks: An active attack strives to alter or damage the data being exchanged in the network there by halting the normal functioning of the network. It basically modifies, fabricates, impersonate and replicate the data.

External attack and internal attacks: These kinds of attacks depends on the domain of the attacks.

External attack: The attacker aims to cause jamming or blockage, propagate fake routing information or disturb nodes from providing services. These kinds of attacks are executed by nodes which are from outside the network.

Internal attacks: The attacker gains the normal access to the network and takes part in the network activities, either by some malicious impersonation to get the access to the network as a new node or by directly compromising a current node and using it as a basis to conduct its malicious behaviors.

Layer based attacks: The attacks can be classified with respect to different layers present in MANET. The attacks are classified as:

- Application layer: Repudiation and data corruption
- Transport layer: Session hijacking and SYN flooding
- Network layer: Wormhole, backhole, Byzantine, flooding, resource consumption and location disclosure attacks
- Data link layer: Traffic analysis, monitoring, disruption MAC (802.11) and WEP weakness
- Physical layer: Jamming, interception and eavesdropping
- Multi-layer attacks: DoS, impersonation, replay and man in the middle

There are many other types of classification in attacks on MANET. Like the stealthy and non-stealthy attacks, cryptographic and non-cryptographic and single and multiple attackers.

Node capture attacks: Passive, active and physical attacks combined together results in node capture attacks. The attacker will collect data's about the network by eaves dropping on message exchanges either restricted to individual attacker device or during the network with the aid of number of attacker devices deployed throughout the network in order to initialize or set up an attack. The attacker can extract data about the network operation and state along with successfully learning about the network structure and function although the message payloads are encrypted.

The attacker can capture a node from the network ultimately acquiring all the cryptographic material stored in it. Also the captured nodes can be reprogrammed by the attacker and redeployed in the network in order to carry out malicious activities. Solution to node capture attacks has to meet the following requirements:

- To detect the node capture as early as possible
- To have a low rate of false positives-nodes which are believed to be captured and thus subject to a revocation process but which were not actually taken by the adversary
- To introduce a small overhead (Conti *et al*., 2009)

In the earlier research (Murugan and Shanmugam, 2010), reaearchers have developed a combined solution for routing and MAC layer attacks. The approach make use of three techniques simultaneously which consists of a cumulative frequency based detection technique for detecting MAC layers attacks, data forwarding behavior based detection technique for detecting packet drops and MAC based authentication technique for packet modification. The combined solution presents a reputation value for detecting the malicious nodes and isolates them from further network participation till its revocation. In this approach, the technique to mitigate node capture attack is not taken into account.

As an extension to the earlier research, researchers developed a cluster based authentication technique to mitigate the internal attacks or node capture attacks. The authentication is performed by the cluster head by checking the trust count value of its members.

LITERATURE REVIEW

Conti *et al*. (2009), proposed a study based on mobility and cooperation to thwart node capture attacks in MANETs. They address the node capture attack in MANETs. The solution is based on the intuition that node mobility together with local node cooperation can be leveraged to design security protocols that are extremely

effective and energy efficient. They have also developed a protocol that increasing the level of cooperation among nodes makes global information flow faster in the network even if at a cost in terms of energy. The experiments clearly show that leveraging mobility and cooperation helps in designing effective and efficient protocols. In particular they also pointed out that there is critical speed necessary to induce enough information flow to make these new protocols outperform traditional ones, designed for static networks.

Chatterjee (2009) proposed a new approach based on trust based self-organizing clustering algorithm. They have used the trust evaluation mechanism depending on the behavior of a node towards proper functionality of the network. The trust evaluation model gives a secure solution as well as stimulates the cooperation between the nodes of the network. The originality of their research consists of combining different metrics for quantifying trust and the use of DS theory in order to predict the trust of mobile node more accurately. In future they plan to compare the proposal with other existing proposals and to consider other issues like secure movement and location management of Individual node to provide a better robust and secured solution.

He *et al.* (2009) proposed a SMOCK scheme which adopts the combinatorial design of cryptographic keys to achieve lightweight key management. They further extend the idea of SMOCK to other applications such as broadcast authentication. Based on the SMOCK idea they design a combinatorial hash-chain sharing scheme: a hash chain pool HC is constructed for the whole network and nodes store the commitment information for all of the hash chains in HC. All of the hash chains have the same releasing schedule which is guaranteed by loosely time synchronization. Message signing and verification use all the hash chains associated with the senders identity. With the combinatorial design, they expect better scalability and less delay than traditional broadcast authentication schemes. They will investigate this deeply in future research.

John and Samuel (2010) proposed enhanced Scalable Method of Cryptographic Key management (SMOCK). They present a clustering based technique to reduce the two drawbacks; to over dependent on centralized server and increase in key-pair when node increases (proportionally less compared to traditional approach) which SMOCK posses. The clustering technique used select a CH is an adaptive weight clustering method. The CH is stored with public keys of all its member nodes. The communication of nodes between two different clusters happens through their CH. Their method also discusses about the effects of node mobility between clusters.

CLUSTERING IN MANET

The entire set of nodes is divided into a number of groups and the nodes inside each group are subdivided into clusters. Each group has a Group Leader (GL) and each cluster is headed by the CH. Specifically, one of the nodes in the clusters is cluster head (Fig. 1).

It is assumed that all nodes communicate via a shared bi-directional channel and operate in promiscuous mode. Using the pair-wise key pre-distribution scheme, keys are distributed over the nodes of the network. A network key is generated by the CHs. There are other keys also for secure communication, 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.

Cluster formation: The following steps have to be performed for electing the CH:

- Step 1: After deployment, the nodes broadcast their id value to their neighbors along with the HELLO message
- Step 2: When all the nodes have discovered their neighbors, they exchange information about the number of one hop neighbors. The node which has maximum one hop neighbors is selected as the CH Other nodes becomemembers of the cluster or local nodes
- Step 3: The cluster head broadcasts the message CLHEAD so as to know its members
- Step 4: Before members reply with the message CLMEMBER they check the available one hop neighbour to ensure that the node the node which has broadcasted the message CLHEAD is actually CH or not. And in this way clusters are formed in the network

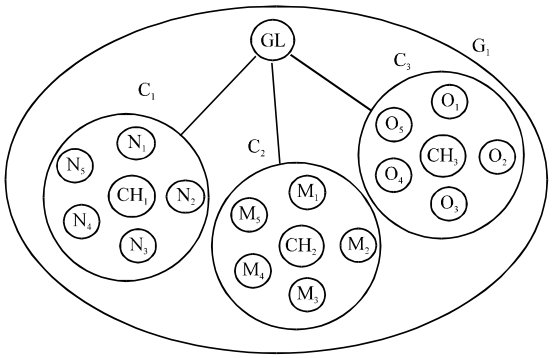

Fig. 1: A typical cluster formation

- Step 5: If a node receives more than one CLHEAD messages it becomes gateway which acts as a mediator between two clusters

Once CHs are deployed each CH starts to communicate between them and they initiate with pair wise key to communicate between each other. Once the nodes are deployed, getting HELLO beacon, any node (while activated) wants to join in the network, sends the public key (preloaded). When any CH gets this message it gives a unique IP address.

In this manner, clusters are formed in the network. The CHs broadcast the message, CLHEAD EXCHANGE so as to know each other. The CH with the least id is chosen as the leader of the CHs which is representative of the group termed as Group Leader (GL). The GLs will be in contact with other GLs in similar way and one among the GL is selected as the leader for entire network. The entire network is hierarchical in nature and following sequence is observed network-group-cluster-cluster members.

Node registration: When a new node wants to join the network, the registration procedure is as follows:

- Step 1: Each CH starts to broadcast CH beacon and attracts some nodes to join its cluster
- Step 2: As the Node M gets the CH beacon it sends JOIN beacon to join the network with its public key
- Step 3: CH checks whether it is a duplicate message or not. If it is not a duplicate, CH stores the public key of M as its id and generates a pair wise shared key to communicate between CH and M
- Step 4: Initially CH gives the node status as Suspicious and allows it to register subject to periodic review

When a node leaves the cluster due to its mobility it does not send any notification to its CH. As the CH maintains the list of its members it can decide whether a particular node has left the cluster or not from the trust table. The trust table gets updated periodically. If any of the node leaves the cluster then its corresponding trust value will not be calculated by other nodes and hence, the trust table entry of that particular node will not be updated. Finally, the CH removes the information regarding the node which has left the cluster.

Trust estimation: Initially, CH sets the status of a newly joined node as suspicious and tries to evaluate the trustworthiness of the node. There are a lot of parameters for determining the trust level of a node. The objective is to devise a mechanism for evaluating the trust of a node according to its contribution towards proper functioning of the network and minimizing the number of misbehaving nodes from the network. Let us now consider the trust evaluation for a node, a packet and a route.

The trust estimation model assist the security model in making decisions for the following contexts such as whether to accept or reject a route from a route discovery to forward or discard a packet, to forward a packet for a previous-hop, to send a packet to a next-hop and which route to choose for the communication. The decision for each context depends on the corresponding trust evaluation. In turn, trust evaluations are based on the direct trust held for one or more nodes involved in the context. A node's direct trust is based on the evidence captured by its security models during the one to one experiences with the other node.

Direct trust estimation: To calculate direct trust, the query node makes use of the following trust parameters. Assume that node A is the query node.

P_f = No. of packets forwarded
P_d = No. of packets dropped
P_m = No. of packets misrouted
P_r = Total no. of packets received by B sent from A

Algorithm for trust calculation:

- Step 1: Collect data for P_f, P_d, P_m and P_r
- Step 2: Find the threshold values associated to each behavior f_n, d_n and m_n
- Step 3: Calculate ratio f_s, d_s and m_s of each behavior and Pr total sent packet accordingly
- Step 4: Calculate the deviation f_d, d_d and m_d from the corresponding threshold:

$$f_s = \frac{f}{P_r} \text{ and } f_d = f_n - f_s$$
$$d_s = \frac{d}{P_r} \text{ and } d_d = d_n - d_s$$
$$m_s = \frac{m}{P_r} \text{ and } m_d = m_n - m_s$$

- Step 5: Calculate the corresponding direct trust value using the equation:

$$\text{Trust} = f_d - (d_d + m_d)$$

Trust certification: Each node calculates the trust value of its one hop neighbors. All the trust values which are estimated are sent to CH periodically. After receiving the calculated trust from each node, CH determines the trust

value of each node by summing all the trust values given by its one hop neighbours. It can be represented as:

$$Trust_{sum} = \sum_{i=1}^{n} Trust_i$$

where, i is the number of one hop neighbours. If the sum of trust value is positive then CH generates the trust certificate to the corresponding node. The CH sends the list of generated trust certificate ode details to all the trusted nodes. By using this trusted node details each node can infer other trusted nodes which can be used for further communication. The trust certificate issued by CH has an expiration time after which again each node has to calculate the trust values of its one hop neighbours.

SECURED ROUTING

Consider that any node having status other than Trusted will not be able to communicate either inside or outside the cluster. Thus the communication is secured. For intra cluster routing, any node is able to communicate to other within the cluster by encrypting the message by the pair wise secret key if two communicating nodes are in broadcast radio range.

Intra cluster routing: Assume that the mobile nodes N_1 and N_2 are in the same cluster under CH_1. If N_1 wants to communicate with N_2 then N_1 will check its trust certificate list issued by CH_1 to decide N_2 is trusted or not.

Algorithm intra cluster routing

- Step 1: N_1 will check its neighbor list. If N_2 is in the one hop neighbor list then it just encrypts the message by the pair-wise key K (N_1-N_2) generated by N_1 and N_2 and sends it to N_2
- Step 2: If it is not, N_1 will ask the CH_1 for the route request. Now CH_1 will checkwhether N_2 is in intracluster or intercluster. If it is in intracluster, CH_1 sends the public key of N_2
- Step 3: N1 generates a key K_s and encrypts K_s with the public key of N_2 and encrypts the message with K_s and sends it to N_2
- Step 4: After getting the message, N_2 sends an acknowledgement via the reverse path

Inter cluster routing: Assume that mobile nodes N_1 and N_2 are in different clusters C_1 and C_3 under the cluster heads CH_1 and CH_3.

Algorithm for inter cluster routing

- Step 1: N_1 sends the route request to CH_1
- Step 2: CH_1 checks the status of the N_1 if N_1 is not Trusted, CH_1 just drops the request and generates a message. If N_1 is trusted, CH_1 generates OK message
- Step 3: Now CH_1 will check whether N_2 is in intracluster or intercluster. If it is in intercluster then CH_1 multicasts canyoufind-N_2 query to all its neighbour CHs for having communication to CH_3
- Step 4: If CH_3 replies or any other CH replies that it can sense N_2 then CH_1 initiates a route discovery request and asks for the public key of N_2
- Step 5: N_1 getting the public key of N_2 from CH_1, generates a key K_s and encrypts K_s with the public key of N_2 and encrypts the message with Ks and sends it to N_2
- Step 6: After a successful receipt N_2 sends an acknowledgement via the same path

MITIGATION OF MISBEHAVING NODES

To mitigate the misbehaving nodes, the direct trust is calculated based on the trust parameters about the neighbor node of the query node. While a query node is getting the information that a node is not forwarding any packet coming to that node or dropped some packets according to the proposed trust model its trust value will be calculated and the same will be forwarded to its CH.

After receiving the periodic trust update from all its members the CH determines whether a particular node is trusted or untrusted based on the majority of trust value given by its neighbours. If the node is marked as untrusted then it is isolated from the network.

Consider a case while a malicious node gets two HELLO beacon from two different CHs. It simultaneously replies to both of the CHs and gets IP and node-id from both the CHs and join under two CHs simultaneously as a legitimate node. IF this node cannot be traced, the whole security structure will be destroyed. As the CH would check packet passing through each node if it finds different packets generated from a node having different IP address or node-ids, the CHs will disconnect the node at once.

As CH gives the unique node-id to its legitimate member nodes and any communication initiated by any node should be identified with the node-id. So, for any malicious node it is impossible to get the legitimate node-id and initiate any intra or inter cluster communication. Thus, impersonation attack can be mitigated.

SIMULATION RESULTS

Simulation model and parameters: Researchers use Network Simulator (NS2) to simulate the proposed algorithm. In the simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. Researchers use the Distributed Coordination Function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. It has the functionality to notify the network layer about link breakage.

In the simulation, mobile nodes move in a 1000×1000 m region for 50 sec simulation time. Researchers have kept the number of nodes as 100. The number of attackers is varied from 5-25. Researchers assume each node moves independently with the same average speed. All nodes have the same transmission range of 250 m. In the simulation, the node speed is 10 m s^{-1}. The simulated traffic is Constant Bit Rate (CBR). The simulation settings and parameters are summarized in Table 1.

Performance metrics: Researchers evaluate mainly the performance according to the following metrics.

Resilience against node capture: Researchers are going to calculate how a node capture affects the rest of network resilience. It is calculated by estimating the fraction of communications compromised between non compromised nodes by a capture of x-nodes.

Average end to end delay: The end to end delay is averaged over all surviving data packets from the sources to the destinations.

Average packet delivery ratio: It is the ratio of the number of packets received successfully and the total number of packets transmitted.

Average packet drop: It is the average number of packets dropped by the misbehaving nodes. The simulation results are presented in the next section. Here the SOR protocol is used in which the comparative study is made with SOR and SOR with proposed scheme CBTM. The performance is evaluated in the process of misbehaving nodes.

Table 1: Simulation settings

Parameters	Values
No. of nodes	100
Area size	1000×1000
Mac	802.11
Radio range	250 m
Simulation time	50 sec
Traffic source	CBR
Packet size	512
Speed	10 m sec^{-1}
Misbehaving nodes	5, 10, 15, 20, 25

RESULTS AND DISCUSSION

Even though the number of misbehaving node increases upto 15, the delay for the proposed system is less because the nodes in either intercluster or intracluster routing are trusted. But as the number of misbehaving node increases upto 20, the probability of discovering trustworthy route decreases considerably due to reduced proportion of CBTM nodes (Fig. 2).

CBTM nodes perform better packet delivery ratio than SOR because it receives packet only from trustworthy nodes and it forwards packet only to trustworthy next hop, using trustworthy intracluster or intercluster routes. Further the result confirmed that CBTM enables nodes to establish valid routes despite of increasing portion of misbehaving nodes (Fig. 3).

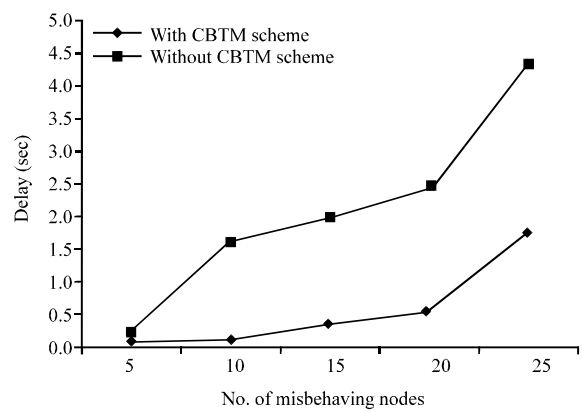

Fig. 2: Misbehaving nodes vs. delay

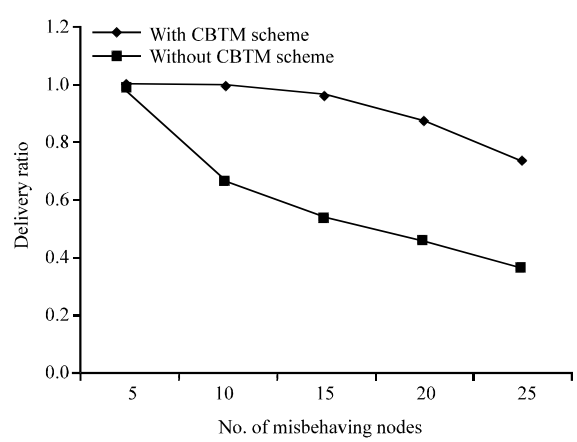

Fig. 3: Misbehaving nodes vs. delivery ratio

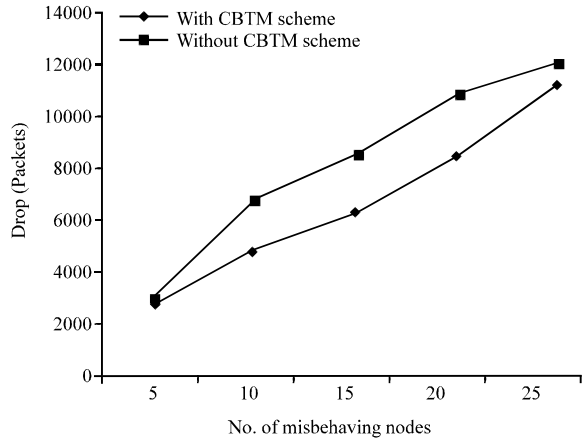

Fig. 4: Misbehaving nodes vs. drop

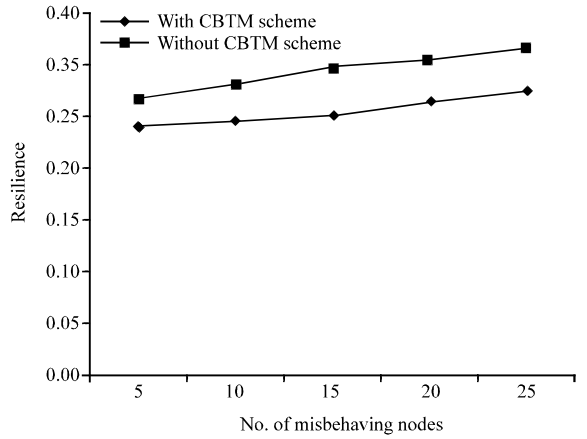

Fig. 5: Misbehaving nodes vs. resilience

Since, the misbehaving nodes are identified by CH and are isolated from the clusters, initially as the number of misbehaving nodes are minimum, the number of packets dropped are minimum. As the number of malicious nodes increases the average packet dropping also increases. But this packet dropping is due to decrease in the probability of discovering the trustworthy route (Fig. 4).

The proposed scheme has higher resilience than the SOR because a trusted environment is created for establishing a route with trusted nodes (Fig. 5).

CONCLUSION

In this study, researchers have developed a Cluster Based Trust Mechanism (CBTM) to mitigate the internal attacks in MANET. In this technique, the entire network is divided into hierarchical group of clusters, each cluster having a fully trusted cluster head. A new node can register or join a cluster and initially the CH sets the status of the newly joined node as suspicious and evaluates the trust of the node. With the direct trust estimation, each node estimates the trust of its one hop neighbour and these trust values are sent to the CH periodically. By summing up all the trust values, CH determines the behavior of the node. The positive trust value shows that the node is well behaving and the CH generates a trust certificate for the corresponding node. The negative value of trust shows that the node is untrusted and it should be isolated from the network. By simulation results it is shown that the proposed technique provides better packet delivery ratio and higher resilience against internal attacks.

REFERENCES

Chatterjee, P., 2009. Trust based clustering and secure routing scheme for mobile Ad Hoc networks. Int. J. Comput. Networks Commun., 1: 84-97.

Conti, M., R. Di Pietro, L.V. Mancini and A. Mei, 2009. Mobility and cooperation to thwart node capture attacks in MANETs. J. Wireless Commun. Network., 10.1155/2009/945943.

He, W., Y. Huang, R. Sathyam, K. Nahrstedt and W.C. Lee, 2009. SMOCK: A scalable method of cryptographic key management for mission-critical wireless Ad-Hoc networks. IEEE Trans. Inform. Forensics Secur., 4: 140-150.

Huang, Y., B. Jin, J. Cao, G. Sun and Y. Feng, 2007. A selective push algorithm for cooperative cache consistency maintenance over MANETs. Proceedings of the 2007 International Conference on Embedded and Ubiquitous Computing, December 17-20, 2007, Taipei, Taiwan, pp: 650-660.

John, S.P. and P. Samuel, 2010. A distributed hierarchical key management scheme for mobile Ad Hoc networks. Proceedings of the International Conference on Information, Networking and Automation, October 18-19, 2010, Kunming, pp: 308-314.

Murugan, R. and A. Shanmugam, 2010. A combined solution for routing and medium access control layer attacks in mobile ad-hoc networks. J. Comput. Sci., 6: 1416-1423.

Orwat, M.E., T.E. Levin and C.E. Irvine, 2008. An ontological approach to secure MANET management. Proceedings of the 3rd International Conference on Availability, Reliability and Security, March 4-7, 2008, Barcelona, pp: 787-794.

Razak, S.A., S.M. Furnell and P.J. Brooke, 2004. Attacks against mobile Ad Hoc networks routing protocols. Proceedings of 5th Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting, June 28-29, 2004, World Scientific and Engineering Academy and Society, USA., pp: 147-152.

Saad, M.I.M. and Z.A. Zukarnain, 2009. Performance analysis of random-based mobility models in MANET routing protocol. Eur. J. Sci. Res., 32: 444-454.

Shanthi, N., L. Ganeshen and K. Ramar, 2009. Study of different attacks on multicast mobile adhoc network. J. Theor. Applied Inform. Technol., 9: 45-51.

Uma, M. and G. Padmavathi, 2009. A comparative study and performance evaluation of reactive quality of service routing protocols in Mobile Adhoc networks. J. Theor. Applied Inform. Technol., 6: 223-239.

Wu, B., J. Chen, J. Wu and M. Cardei, 2007. A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks. In: Wireless Mobile Network Security, Xiao, Y., X. Shen and D. Du (Eds.). Springer, New York, pp: 103-136.

Xiao, Y., X. Shen and D.Z. Du, 2007. Wireless Network Security. Springer, New York, ISBN-13: 97803872-80400.