An Introduction to Cloud based Interactive Routing Protocol for Mobile Adhoc Networks (MANETs)

Priynak Kansal[1], Rajender Kumar[2]
[1, 2] CSE Department
[1, 2] HCTM, Kurukshetra University Kurukshetra, Haryana, INDIA

Abstract- *Mobile Ad-hoc Network is a wireless network with self-configuring nodes which forms a temporary network without any centralized administration such as servers and base stations. One of the most critical issues in these networks is the deployment of adaptive, extensible and flexible authentication and access control policies. Moreover, the lack of structured hierarchy in MANETs complicates the overall task of implementing these policies. The network performance might be improved if the network is clustered by grouping together nodes that are in close proximity. In the present paper our primary goal is to provide both an adaptive authentication system and a clustering scheme for MANET keeping the clustering latency, cost and performance in mind.*

Keywords- Multi-hopping, Farthest Node Selection, FRENSA, EPSAR, Routing, Cloud, Fair Routing

I. INTRODUCTION

Mobile ad hoc networks are such kind of network that works under dynamic routing with mulihopping mechanism and have no centralized body to govern the network under which the network has to communicate. Apparently it's crucial to work with such kind of network because of the absence of base stations/routers. In MANETs nodes itself have capability to act as base station/router and every node may function as a router and forward packets through routing paths. Co-operation among nodes during path discovery and packet relaying is of primary concern and should be supported for correct functioning of the network. Communication in a MANET occurs in a discrete and disperse environment with no centralized management which arises a main issue in MANET that is the breakage of link at certain moment and re-generation of link at certain state. In order to work with MANETs we have some predefined routing strategies through which we can pursue our communication i.e. active routing (on demand), proactive routing (table driven). Rest of these there is one more routing strategy known as preemptive routing (works on the bases of signal strength and age of path) all these strategies have their own pros and cons. All these protocols have some excellent features if we intermingle all these features especially give more emphasis on signal strength that acts as threshold and we could lead towards a routing path that is highly efficient in terms of power consumption too. [1], [2]

The mobile ad hoc network (MANET) is established by a group of mobile and independent nodes connected by wireless links. These associated hosts are independent to roam in an arbitrary motion. The unavailability of controller coupled with the frequent changes in the network topology makes network functions or services in MANET much complicated as compared to that in any other network. The structure of mobile ad hoc network is decentralized and communicating nodes are heterogeneous; some nodes may have different processing capabilities and battery power. The nodes are responsible of not only forwarding packets for other nodes but also perform extensive computation. These computations can be in terms of route maintenance, key management and the deployment of security schemes. The transmissions and computations cause the resources to be depleted. Therefore, to avoid a node dropping out of the network prematurely, the overhead of all the activities and deployed schemes should be kept to a minimum. To deal with the random entries of nodes, security mechanisms need to be robust and flexible to some extent. [2,7]

II. AUTHENTICATION SCHEME

The insertion of a new node starts with persuading a legitimate node. The non-legitimate node requests for its insertion into the network through a request message which includes its node ID, sequence number, off line period and body of proof. Sequence number is included so as to identify multiple requests from the same node and to avoid the loops. The legitimate node checks for the node-id, whether the ID carried by this non-legitimate node is unique in its close proximity or not. This legitimate node investigates the past behavior of it before allowing this node for the services of the network. Investigation includes the information regarding the nodes' mobility and its co-operation in the network operations.[4]

The algorithm needs to ensure the exclusion of malicious and selfish nodes. Misbehaving nodes do not co-operate in the network operations either intentionally as they

conserve their resources or unintentionally, when do not have the sufficient resources to participate in the network operations. The legitimate node forwards the investigation message (INVES_MSG) to its neighbors (i.e. to the nodes in its transmission range). This broadcasting of messages is the limited broadcasting i.e. the packets are flooded to the neighboring nodes. Upon receiving the INVES_MSG neighbor nodes checks their locally maintained information to detect the routing pattern followed by the requesting non-legitimate node earlier. The replies (INVES_REP) are collected and further analyzed at the node from where the INVES_MSG originated. The performance and reliability of the requesting or non-legitimate node are the two important parameters which decide their legitimacy.[12]

Request message from the non- legitimate node

NODE_ID	SEQ_NO.	OFFLINE_PERIOD	BODY_OF_PROOF

Figure 1. Request Message Packet

Sequence number information (SEQ_NO.) eliminates the formation of loops in the network and to differentiate between the recent and the stale requests. Offline_period denotes the time interval when the node is out of coverage. If a node has been off-line and wants to connect on-line, it has to contact a legitimate node who checks whether the off-line period is not greater than Θ, where Θ (theta) denotes a predefined time interval which depends on the number of nodes, computing power of nodes and the connections bandwidth. Body_ of_ proof is to confirm the presence of all the legitimate nodes in an active way by broadcasting their body of proofs every certain interval of time to all the legitimate nodes.

1. Legitimate requested node checks the information

if ((OFFLINE_PERIOD < Θ) && (SEQ_NO. = unique))
Allow the node
else if((OFFLINE_PERIOD > Θ) && (SEQ_NO. = unique))
Send INVES_MSG

NODE_ID	SEQ_NO.	OFFLINE_PERIOD	MSG_SEQ_NO.

Figure 2. Investigated Message Packet

else discard the request

2. For every neighbor node process INVES_MSG

a) For the given node ID check the mobility and the routing patterns.
b) INVES_REP is forwarded to the node which initiated the INVES_MSG.

3. After receiving enough replies carry out a probabilistic analysis.

4. Send a reply message to the requesting node. Send the topology information to the node if it is legitimate now.

5. Re-evaluate the body of proof for every node in the network after T time interval.

Where: T depends upon the no. of nodes and throughput of the network.

- Cost = No. of messages involved * length of each message.
- Authentication latency= Delay between the time when the request message was sent and the time when the node receives the reply.
- Body of proof= Mobility information and the no. of routes through this node to the no. of packets delivered.

III. CLUSTERING: FORMATION OF CLUSTER AND DESIGN PARADIGMS

Due to the unavailability of a central controller and limited battery power, a flat structure may not be the efficient organization for routing between nodes in the case of large MANETs. One of the way support efficient communication and improved system performance is to develop wireless backbone architecture. Such networks may be logically represented as a set of clusters by grouping together nodes that are in close proximity. The formation of clusters and the organization of nodes in such a manner, with a view to improve the efficiency of routing, incurs low cost in terms of the resources used such as bandwidth, battery power, computation power etc. the purpose of clustering may be defeated otherwise. Certain nodes are elected to form the wireless backbone. These nodes are called Cluster heads and Gateways while other nodes work as member nodes.[3]

A Cluster head serves as a local co-coordinator for its cluster and vested with the responsibility of routing, data forwarding and so on, for all the nodes within its cluster. Gateways nodes are the nodes at the fringe of a cluster within inter-cluster links and access the neighboring cluster to

forward information between clusters. A neighboring cluster is accessed through the gateway nodes.

A cluster member is a node other than a cluster head. It might behave as a cluster gateway if present at the boundaries of the cluster. These member nodes form the communication links within a cluster and may access Cluster head for its services. The Clusters are either deployed with proactive routing scheme or a reactive routing scheme and thus operates accordingly. Nodes are powered by limited batteries because of their mobile nature. Cluster head is involved in every communication within its cluster, so the amount of communication should be kept to a minimum to avoid a node to be dropped out of the network prematurely. The bottleneck to the functioning of a cluster head must be eliminated.

IV. THE DESIGN PARADIGMS FOR BUILDING AN OPTIMIZED CLUSTERED ARCHITECTURE

1. Reliable inter-cluster links:

Once the connections are set up, the effects of mobility of nodes should be kept at minimum. Higher node mobility results in high cost due to the reconfigurations. Mobility based and weighted clustering scheme have been proposed which supports the formation of highly connected intra-cluster links and takes mobility as the metric for cluster formation. The nodes moving with same velocity are grouped together to form a cluster, but the velocity with which the node moves is not the only factor to consider, their direction of movement also has important concerns. Cluster formation and maintenance are expensive tasks for the nodes so there should be minimum re-configurations and re-affiliations when a node detach from one cluster and attach to another.[5]

2. Low Cluster head overhead:

The Cluster head dissipates more power as compared to any other node in the cluster since all the inter-cluster packet forwarding and routing happen through it. The life span of a Cluster head is shorter than the rest of the member nodes. To avoid its premature elimination from the network, the work load should be minimized. One of the proposed self organized clustering schemes includes the use of a proactive routing protocol such as DSDV within the cluster. The cluster formation and maintenance can be handled using member nodes as each node has its proactively maintained routing information with it. This lowers the overhead of explicit message passing through the cluster head.

3. Low Cost:

The cost in Mobile ad hoc network is determined by the power consumption and message overhead during the construction of a cluster and its maintenance. Energy is a critical resource for every node. A simple cluster formation algorithm begins with the selection of the neighbors for each node (i.e. nodes within its transmission range). Each node diffuses its identity through a HELLO message which is recorded by all the other nodes. This process repeats for all the nodes not yet assigned to any cluster. Moreover, due to the dynamic nature, the nodes and the Clusterhead tend to move in random directions causes a disorganization of the network configuration. Thus the system must be updated from time to time. The communication overhead tends to increase in the lack of an efficient scheme.[10]

4. Low Cluster latency:

The formation of a cluster and the election of a clusterhead require co-ordination among the mobile nodes. The implemented scheme ensures a minimum latency while forming the clusters. When a node send a request message there occurs a specific delay in receiving a reply message. Also the election of clusterhead puts a significant overhead. All the parameters for the selection of a clusterhead must be evaluated first, and then the cluster ID (CID) is forwarded to all the member nodes. Due to the lack of central entity, mobile node experiences certain delays. This issue has been of considerable interest in the network research community when it comes to infrastructure less networks. Large cluster latencies degrade the throughput and efficiency of the system.[13]

5. Self organization:

Completely distributed nature and the absence of a centralized infrastructure make it difficult to control the topology of Ad hoc networks. Thus the network is divided into clusters, which has made the situation less complicated. A self organized and self configurable system is one which organizes itself without any external or central dedicated control entity. Self organization is one of the prominent features of a clustered architecture. One of the proposed self organized approaches to MANET clustering includes the use of a proactive inter-cluster routing protocol. Whenever a new node joins the cluster it starts advertising itself and all nodes in its cluster will have an entry for this node in their routing tables after a short time. The system activation and update policies works in two cases:

- When reviewing cluster formation
- When a node changes its affiliations from one Clusterhead to a new one.

V. VULNERABILITIES AND PROBABLE SOLUTIONS TO SECURE ROUTING IN MOBILE AD HOC NETWORKS (MANETS)

1. Link unreliability:

The correct operation of the network requires not only the correct execution of the network functions but also some schemes to cope up with dynamically changing network topology. A link no longer participates in a packet forwarding process because of its corresponding node movement and limited resources which causes havoc in the network as the routing suffers an interruption, nodes have to retransmit the lost packets, and network has to reconfigure the path to the destination.

Solution: Computation of link reliability as safe or unsafe. The havoc caused by several link breaks can be controlled, if we priory estimate its reliability and associate a trust level accordingly. To implement this idea, a node must be issued with an off-line certificate by several other nodes in the network, on the basis of its behavior like its mobility and resource availability.

2. Bandwidth constraints:

Unlike the wired counterparts the networking scenario is far more distributed in nature in mobile ad hoc wireless network, which adds a substantial responsibility upon the nodes. In such environment the optimal utilization of the bandwidth among nodes is not expectedly supported. Thus the limited capacity of radio band to offer data rates becomes a challenge in mobile ad hoc networks.

Solution: Adaptive protocols. To countermeasure the effects caused by the bandwidth constrained ad hoc network, an adaptive scheme must be deployed. Forwarded data packet is embedded with some information regarding the bandwidth it requires for its relaying and processing. The intermediate/destination nodes check this requirement and then take an action accordingly.

3. Resource Limitation:

Various routing, packet forwarding, service discovery and security schemes adopted by each device in the network has to work within its own resource limitations in terms of computation capabilities, memory , communication capacity and energy supply. The battery power/energy carried by a mobile node has limited energy and processing power which leads to the support for limited number of applications and services.

Solution: Reduce the overhead. The scarcity of resources within a network causes denial of services, which can be overcome by enabling a node to set a threshold value for its processing power, battery, communication capabilities and other resources. When a node receives a packet, it checks its threshold limit, if the node does not find itself able to process that packet; it chooses some of its neighbor nodes to process that packet. It maintains a queue, when data traffic is high in the network.

4. Route maintenance:

Mobile hosts in mobile ad hoc network usually move freely, which causes the topology of the network to change dynamically and disconnection occurs frequently. The nodes take advantage of the multihoping nature of the mobile ad hoc network and search for an alternative path to the destination for the data transfer. But the data sent by the source node during alternate path establishment period will be lost leads to incomplete data transfer and thus become responsible for a considerable increase in network traffic because of the retransmission of the data after re-establishing the link.

Solution: Conventional routing protocols integrate route discovery with route maintenance by continuously sending periodic routing updates to other nodes in the network. If the status of a link or a node changes, the periodic updates will eventually reflect the changes in all other nodes presumably resulting in the computation of the new routes to the destination nodes. The route maintenance approach adapted by the preemptive routing scheme involves the routing algorithm to discover an alternative path before the breakage of the actual link. Thus improves the network connectivity. This approach is similar to the soft handoffs in mobile telephone networks.

5. Network partition:

The routing protocols being implemented in adhoc environment sometimes do not cope with network partitions; as a result a set of nodes behaves independently of others. This sort of partitioning affects the performance badly and has severe consequences which includes non optimal routes and loss of data etc.

Solution: Network partition mainly occurs due the node movement and thus the other nodes which were connected to this moved away node suffers a disconnection with the rest of the network. The connection can be again established through periodic sending of beacon messages or through predicting the node movement and link breakage.

6. Hidden Terminal Problem:

The data transmission from sender to receiver, sometimes suffers a sudden interruption collision due to the simultaneous transmission from these nodes, which are not within the direct transmission range of receiver. These nodes are considered as the hidden nodes as they start transmitting data at the same time, unaware of the data transmission from other nodes to the same destination. The shared wireless link does not allow this type of transmission to take place which results in collision and packet loss. Hidden terminal problem degrades the system performance and throughput and needs to be alleviated.[6]

Solution: The collision among data packets during the transmission from the hidden nodes can be avoided if a priority assigning scheme is employed with in the network for various cells to which the communicating nodes belong. When a node receives the data packets from other multiple hidden nodes (i.e. the nodes which belongs to different cells or clusters) it checks the priority or preference level of the cell this sending node belongs to and acknowledge it accordingly. Thus this priority wise servicing of multiple hidden nodes can eliminate the chances of collision among the packets

.

7. Exposed terminal problem:

Exposed terminal problem prevents a node from transmitting data when a nearby node (in the direct transmission range) occupies the wireless channel to transmit packets to the destination node. The alleviation of this problem needs some synchronization mechanism to be established among the nodes in the network, so that the throughput cannot be affected during high traffic loads. Nodes overhear the channel and starve themselves until the other node which belongs to the same cell as that of the overhearing nodes continue transmitting packets.

Solution: Exposed nodes, which are prevented to transfer their data because of the ongoing data transmission from one of their neighbor node, if assigned a priority or preference by the receiving node, can alleviate this problem. The receiving node makes a check over the priority of the sending node and acknowledges it according to that preference level it is assigned with. So the exposed nodes need not prevent themselves to send data over the shared channel. It's the receiving node who manages the priorities considering the various parameters.

8. Non-optimal routes:

The inconsistent routing information, regular movement of nodes and malicious modification of routing information by an attacker results in the formation of non-optimal routes in the network for traffic forwarding. In a highly dynamic environment, where nodes keep on changing their positions, the other connected nodes have to search for new paths, which are not guaranteed to be optimal. A malicious node attacks the network links and modifies the routing data being transmitted over that link.[8]

Solution: Modified algorithm for the selection of path to the destination. The nodes in the network uses algorithm like Dijkastra and many more to search minimum length or shortest path to the destination to route their packets. If an adversary has managed to detect all the information regarding the network and its nodes behavior then it can easily find out the shortest path through which a node is communicating with the other node. The malicious node then attacks that link and the traffic transmitted along that link becomes compromised. If this approach is extended by following the second shortest path to the destination rather than the first shortest path then the attacker will not be able to contaminate the data transmission.

9. Unpredictable connectivity:

If a mobile node in MANET want to transmit data packets to the rest of the network then it requests its neighbor node for their co-operation to detect the routes and then to relay the packet. If a node deny forwarding it then the given source node request some other nearest and node for the same purpose. Moreover the node movement and scarcity of resources at nodes affects the connectivity. This unpredictability in establishing a connection with other nodes results in the delay and the formation of non-optimal paths in the network.

Solution: Integrate Mobile ad hoc networks with Artificial intelligence and neural networks. If a network is made to operate intelligently, which can predict its future connectivity with other nodes on the basis of its learning and training then it would be far more easy for a mobile node to detect its efficient and optimal paths to the destination with no or small delays. Mobility of nodes is the biggest hindrance in the path of network training. The maintenance of broken links, QoS, traffic management, provisioning of security, location discovery, congestion control, measurement of resources etc. can be handled effectively if the network is well trained.

VI. CONCLUSION

The inherent lack of the infrastructure and open nature of mobile ad hoc networks, information routing and security exposures can be an impediment to basic network operation and countermeasures should be included in the network functions from the early stages of design. The above proposed solutions for certain vulnerabilities have to cope with a challenging environment including scarce energy and computational resources and lack of persistent structure to rely on for building trust. These solutions only cover a subset of all the vulnerabilities and are far from providing a comprehensive answer to the routing and security problems in MANETs. The routing proposals do not take into account lack of co-operation and do not include co-operation enforcement schemes.

REFERENCES

[1] P. Caballero-Gill, C. Caballero-Gill, J. Molina-Gill, and A. Quesada-Arencibia, “A Simulation Study of New Security Schemes in Mobile Ad-Hoc NETworks”, ©Springer-Verlag Berlin Heidelberg 2007.

[2] Nevadita Chatterjee, Anupama Potluri and Atul Negi, “A Self-Organising Approach to MANET Clustering”.

[3] Rachida Aoudjit, Mustapha Lalam, Abdelaziz M’ zoughi, “Load Balancing: An Approach Based on Clustering in Ad Hoc Networks”, ©Journal of Computing and Information Technology, 2009.

[4] C.Siva Ram Murthy & B.S Manoj, “Mobile AdHoc Networks- Architecture & protocols”, Pearson Education, New Delhi, 2004.

[5] R. Pandi Selvam and V.Palanisamy, “Stable and Flexible Weight based Clustering Algorithm in Mobile Ad hoc Networks”, International Journal of Computer Science and Information Technologies, Vol. 2 (2) , 2011,824-828.

[6] Ajay Jangra, Nitin Goel & Priyanka "Efficient Power Saving Adaptive Routing Protocol (EPSAR) for MANETs using AODV and DSDV: Simulation and Feasibility Analysis" in IEEE, IPTC 2011

[7] Vasiliou, A., Economides, A.A.: Evaluation of multicasting algorithm in MANETs. In: Proceedings of World Acadmy of Science, Engineering and Technology, vol. 5 (April 2005); ISSN 1307-6884

[8] Y.C. Hu, A. Perrig and D.B. Johnson, “Packets leashes: a defense against wormhole attacks in Wireless networks”, in proceedings of the 22nd Annual Joint Conference on the IEEE Computer and Communications Soieties, vol. 3, pp. 1976-1986, San Francisco, Calif, USA, March-April 2003.

[9] Atef Z. Ghalwash, Aliaa A. A. Youssif, Sherif M. Hashad and Robin Doss, "Self Adjusted Security Architecture for Mobile Ad Hoc Networks (MANETs)" 6th IEEE/ACIS, ICIS 2007, IEEE

[10] Feng Li and Jie Wu, "Authentication Via Ambassadors: A Novel Authentication Mechanism In Manets" by NSF grants CNS 0422762, CNS 0434533,CNS 0531410, and CNS 0626240.c 2007 IEEE.