Volume 2, No. 5, May 2011

Journal of Global Research in Computer Science

ISSN-2229-371X

RESEARCH PAPER

Available Online at www.jgrcs.info

VULNERABILITIES AND SOLUTIONS: MOBILE AD HOC NETWORKS (MANETs) FOR OPTIMAL ROUTING AND SECURITY

Shruti Sangwan[*1], Ajay Jangra[2] and Nitin Goel[3]

[*1, 2, 3] CSE Department UIET, Kurukshetra University, Kurukshetra, Haryana, India
ssshrutisangwan8@gmail.com[*1], er_jangra@yahoo.co.in[2] and goelnitin0887@gmail.com[3]

Abstract: This paper present the impact of some of the unique characteristics, like shared wireless medium, stringent resource constraints, highly dynamic network topology, and peer to peer, multi-hop autonomous network architecture, of MANETs from a wide perspective. These additional features never come for free as they make the routing and other services more challenging and causes vulnerabilities in network services. Resource constrained, battery powered wireless mobile nodes not only have to self configure and self monitor them but also generates a very accommodating, trustworthy and affable environment. Recent advances in wireless networks have led to enhance existing protocols specifically designed for mobile ad hoc networks. We present a classification of routing protocols and their brief description, based on their operating principles and underlying features.

Keywords: Mobile Ad-hoc Networks (MANETs), Multi-hopping, Vulnerabilities, Routing, Security, Preemptive Routing.

INTRODUCTION

Extending mobility into self organized and wireless domains is the main objective of MANET, where a set of nodes form the network routing infrastructure in an ad hoc fashion. The nodes in mobile ad hoc network have self configuring and self monitoring capabilities without necessarily relying on a fixed infrastructure. MANET offers a friendly and co-operative environment with no centralized place where traffic monitoring or access control mechanism can be deployed. Unlike the wire line networks it poses some unique characteristics such as shared wireless medium, stringent resource constraints, highly dynamic network topology, and peer to peer and multihop autonomous network architecture. From the security design perspective, the lack of a clear line of defense is one of the distinguishing characteristic. The network connectivity between the nodes in MANET is provided over potentially multi-hop wireless channel mainly through link layer protocols that ensures single hop connectivity and network layer protocols that extend the connectivity to multiple hops. But the multi-hopping capabilities of these MANETs suffer in the case where a large number of nodes are operational, triggering a deterioration in the network's performance. [1]

In MANETs 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 as it consists of routers which are mobile in nature i. e. are independent to roam in an arbitrary motion.

A MANET is a dynamic multi-hop wireless network which is established by a group of mobile and independent nodes on a shared wireless channel by virtue of their proximity to each other. Generally low configured nodes are used in mobile adhoc networks to support mobility to user, so limited resources, dynamic network topology and link variations are the major issues with MANET. The number of link breakages observed by a node in an adhoc network can be used as a mobility metric so that each individual node can adjust its routing behavior based on the environment around it which improves the overall routing protocol performance.[4]

Ad hoc networks should give more emphasis and should also meet the following requirements to support a wide range of applications including military operations, outdoor emergencies, and natural disasters. [2, 5]

1. *Scalability:* The routing protocols employed for packet forwarding should be capable to scale for a network with a large number of nodes where the nodes keep on adding into the network dynamically. Routing should efficiently adapt itself to the network size.

2. *Distributed Nature:* The routing, computation and maintenance approaches in an adhoc wireless network should be fully distributed as a centralized approach in these domains may consume a large amount of bandwidth.

3. *Communication Capabilities:* The lack of any centralized support should not hinder the communication among the nodes.

a.) Fault Tolerant communication capabilities: The communication links must be able to recover and reconfigure quickly from the potentially induced mobility breaks, thus making it suitable for the use in highly dynamic environments.

b.) Real Time communication capabilities: Mobile adhoc networks employed in certain applications like real time video and voice conferencing, electronic classrooms, multimedia applications demands support for time sensitive real time communication.

4. Flexibility: Adhering to a same set of nodes to a destination throughout the routing process isn't supposed to be valuable. Freedom to select suitable nodes in terms of their reliability and computing power offers flexibility in the network.

5. Efficient Routing: The prerequisites of an efficient routing scheme are the involvement of a minimum number of nodes in route discovery and maintenance and minimum connection set up time. The multicasting of packets should make a minimum number of transmissions to all the group members.

6. *Bandwidth and Resource Availability:* The shared wireless link and stringent resources like transmission power, battery energy, processor power and device power must assure their maximum availability to cope up with such a dynamic environment.

7.Multifence Security Scheme: A multi-hop connectivity is provided in Manets through distributed protocols in both the network and link layers, the ultimate multifence security solution must span both layers with each layer contributing to a line of defense.

The multi-hopping behavior of MANETs is as shown in figure 1. The routing information and data packets travels from one hop hop to another in the network, if a node A wants to send a data packet to node D, it can do so via B which is in the common range of both the nodes. However if B moves away and is beyond the range of A , the link is broken and a different route has to be established.

STRATEGIES FOR ROUTING IN MOBILE AD HOC NETWORKS (MANETS)

The most important networking operations include efficient routing and adequate network management. Based on the routing information update mechanism, ad hoc wireless network routing protocols can be classified in three major categories [3,7]. These are:-

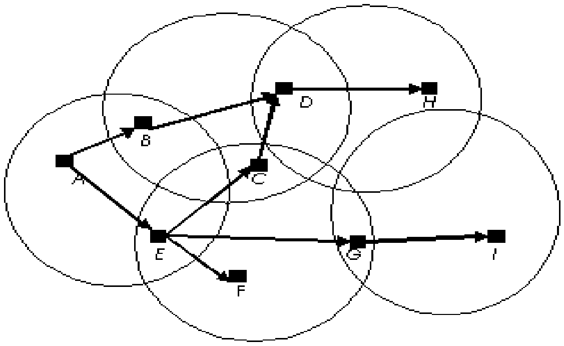

Figure 1. Multi-hopping behavior of nodes in Mobile Ad Hoc Networks

1. Proactive or Table driven Routing

In table driven routing protocols every node in the network maintains routing information and periodically exchange it with other nodes, which add a subsequent overhead in the network as the routing information is generally flooded in the whole network. Sequence numbers are used to distinguish recent information from the stale data. This category of routing suffers from excessive control overhead and keeps on increasing as the network scales to larger number of nodes and when the environment is highly dynamic. The nodes exchange the routing information either through incremental updates or in full dumps. Destination sequence distance vector (DSDV), wireless routing protocol (WRP) belongs to this category and offers availability of routes.

2. Reactive or On demand Routing

Reactive protocols obtain the necessary path to the destination only when it is required uses a connection establishment process. The routing information is propagated to the nodes only when necessary. Reactive protocols out performs proactive ones but high mobility in the network leads to degradation of performance. These protocols eliminate the need to periodically flood the network with table update packets and thus control the bandwidth requirement. The control overhead becomes low if we limit the search area for finding a path to the destination. Adhoc on Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) are the quintessence of reactive routing.

3. Hybrid Routing

Hybrid routing supports dynamic switching between the reactive and proactive parts of the protocol and thus make use of the best features of the above two categories. By combining the best features of proactive and on demand routing scheme, hybrid routing reduces the control overhead compared to the routing request flooding mechanism employed in reactive approach and periodic flooding of routing information packets in proactive approaches. Hybrid routing sometime fails to form an optimal path to the destination node. Core Extraction

Distributed Adhoc routing protocol (CEDAR) and Zone routing protocol (ZRP) falls under the category of hybrid routing based protocols.

PREEMPTIVE ROUTING

One of the efficient routing scheme is preemptive routing where an alternative path is established when the existing path is more likely to be broken by sending a warning message to the source indicating the likelihood of a disconnection which leads to an improved network connectivity. Age of the path and the signal strength are the two parameters which are adopted to compute the reliability of the links a prior. If a same set of nodes participate in the data transmission, then there are chances of these nodes failing because of their resource drain. This helps in computing the age of the path parameter and accordingly an alternate path has to be discovered to avoid the total drain. The second parameter, signal strength, estimates the node's ability to converse with other nodes. This method increases the network traffic required for new path discoveries and signal variations due to fading and other temporary disturbances may generate erroneous results. [4]

**All of these existing routing strategies are responsible for following metrics: Minimizing end-to-end delay, Maximizing end-to-end throughput, adaptable to dynamic topology and Packets are always routed through optimal path*

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 packet to 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.

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]. Hao Yang, Haiyun luo, Fan Ye, Songwu Lu and Lixia Zhanng, "Security on Mobile Ad Hoc Networks: Challenges and Solutions" 1536-1284/04/IEEE Wireless Communications Feb. 2004.

[2]. C.Siva Ram Murthy & B.S Manoj, "Mobile Ad Hoc Networks- Architectures & Protocols" , Pearson Education, New Delhi, 2004.

[3]. Ajay Jangra, Nitin Goel, Priyanka, Komal, "Security Aspects in Mobile Ad Hoc Network (MANETs): A Big

[4]. Picture", International Journal of Electronics Engineering, 2(1), 2010, pp. 189-196.

[5]. Amit Goel, A.k.Sharma, "Security Trends in Wireless LAN".

[6]. Refik Molva and Pietro Michiardi, "Security in Ad hoc Networks"

[7]. Amit Goel, A.k.Sharma, "Secure Communication in Mobile Ad Hoc Network"

[8]. B. R. Sujatha, M V Satyanarayana, "Improved Network Connectivity in MANETs", International Journal of Computer Networks & Communications (IJCNC),Vol.1,No.3,October 2009

[9]. Frank Kargl, Andreas Klenk, Stefan Schlott, and Michael Weber, "Advanced Detection of Selfish or Malicious Nodes in Ad Hoc Networks", Springer-Verlag Berlin Heidelberg 2005

[10]. Binod Vaidya, Sang-Soo Yeo, Dong-You Choi , Seung Jo Han, "Robust and secure routing scheme for wireless multihop network" Published online: 4 April 2009, in Springer-Verlag London Limited 2009

[11]. Yu Wang, Weizhao Wang, Xiang-Yang Li, "Distributed Low-Cost Backbone Formation for Wireless Ad Hoc Networks" MobiHoc'05, May 25–27, 2005, Urbana-Champaign, Illinois, USA. Copyright 2005 ACM 1-59593-004-3/05/0005