International Journal of Computer Theory and Engineering, Vol. 1, No. 3, August, 2009
1793-8201

Secured Routing Scheme for Adhoc Networks

Ashwani Kush, P. Gupta and C.Jinshong. Hwang

***Abstract*— A recent trend in Ad Hoc network routing is the reactive on-demand philosophy where routes are established only when required. Most of the protocols in this category are not incorporating proper security features. The ad hoc environment is accessible to both legitimate network users and malicious attackers. It has been observed that different protocols need different strategies for security. The proposed scheme is intended to be incorporated on the Power Aware Virtual Node Routing Protocol to protect its routing strategy. The study will help in making protocol more robust against attacks and standardizing parameters for security in routing protocols.**

***Index Terms*— Ad hoc networks, Routing protocols, Security, Secure PAVNR**

I. INTRODUCTION

An Ad hoc wireless network is a collection of mobile devices equipped with interfaces and networking capability. It is adaptive in nature and is self organizing. A formed network can be de-formed and again formed on the fly and this can be done without the help of system administration. Each node may be capable of acting as a router. Applications include but are not limited to virtual classrooms, military communications, emergency search and rescue operations, data acquisition in hostile environments, communications set up in exhibitions, conferences and meetings, in battle field among soldiers to coordinate defence or attack, at airport terminals for workers to share files etc. Although security has long been an active research topic in wired networks, the unique characteristics of Ad Hoc networks present a new set of nontrivial challenges to security design. These challenges include open network architecture, shared wireless medium, stringent resource constraints, and highly dynamic topology. Consequently, the existing security solutions for wired networks do not directly apply to the Ad Hoc environment. The main goal of the security solutions for an Ad Hoc network is to provide security services, such as authentication, confidentiality, integrity, anonymity and availability to mobile users [12]. One distinguishing characteristic of this network from the security design perspective is the lack of a clear line of defense. Unlike wired networks that have dedicated routers, each mobile node in an ad hoc network may function as a router and forward packets for other peer nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. In such an environment, there is no guarantee that a path between two nodes would be free of malicious nodes, which would not comply with the employed protocol and attempt to harm the network operation.

A new scheme has been proposed here to incorporate security features in ad hoc networks. The scheme takes care of basic security needs and uses concept of Hash Key generation to attain the goal of security. The scheme has been incorporated on the refined version of AODV [4], named as PAVNR [2] called power aware virtual node routing protocol. PAVNR embeds the function of power and virtual nodes factor in AODV and improves its performance to achieve more stable routes. Rest of the paper is organized as: Section 2 describes types of security attacks, related work is described in Section 3, Section 4 deals with security model with its impacts, Section 5 is proposed scheme and Section 6 concludes the study

II. SECURITY ATTACKS

In this paper, the prime concern is with the attacks targeting the routing protocols for Ad hoc Networks. These attacks can be broadly classified into two main categories as: Passive attacks, Active attacks.

A. Passive attacks

Passive attacks are the attacks in which an attacker does not actively participate in bringing the network down. An attacker just eavesdrops on the network traffic as to determine which nodes are trying to establish routes, or which nodes are pivotal to proper operation of the network and hence can be potential candidates for subversion and launching denial of service attacks. The attacker can then forward this information to an accomplice who in turn can use it to launch attacks to bring down the network. The nature of attacks varies greatly from one set of circumstances to another. Some of the generic types of attack [16, 19] that might be encountered in passive attacks are:

1. Interruption: An asset of the system is destroyed, becomes unavailable or unusable. This is an attack on availability. Examples include destruction of a piece of hardware, or cutting of a communication line.
2. Interception: An unauthorized party gains access to an asset. This is an attack on confidentiality. The unauthorized party could be a person, a program or a computer. Examples include wiretapping to capture data in a network or the illicit copying of files.

Manuscript received April 10, 2009. This work is supported by the U.G C. Project on security in ad hoc networks under Grant F-2(74)/2008/MRP/NRCB.

Ashwani Kush is working as head of Dept Univ college Kurukshetra University India. He is member of IEEE, ACM, CSI, IACSIT.

P. Gupta is Professor in Comp sci and engg, with Indian Institute of Technology Kanpur, India.

C. Jinshong Hwang is Professor computer science, with Texas state University USA.

3. Modification: An unauthorized party tampers with an asset. This is an attack on integrity. Examples include changing values in a data file or modifying the contents of a message being transmitted in a network.
4. Fabrication: An unauthorized party inserts malicious objects into the system. This is an attack on authentication. Examples include the insertion of spurious messages in a network or the addition of records to a file.

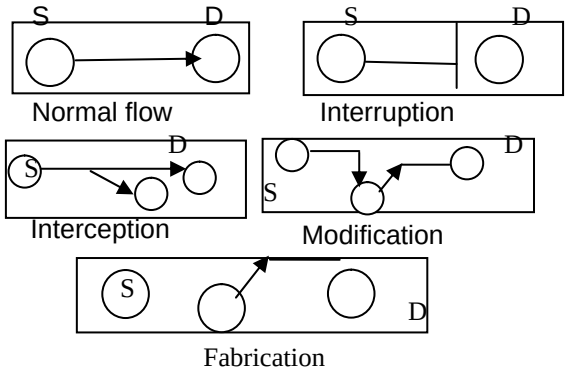


Figure 1: Types of passive attacks

Figure 1 represents type of passive attacks, S represents Source and D represents Destination.

B. *Active* attacks

These attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories.
1. Replacement: In this attack one entity pretends to be a different entity. A type of **attack** that is used by someone familiar with your security procedures and failures. An impersonate attack usually includes one of the other forms of active attacks.
2. Replay: This involves capture of data units and its subsequent retransmission to produce an unauthorized effect. Sniffers are used for legitimate network management functions.
3. Modification of Messages: This simply means that some portion of a legitimate message is altered, delayed or reordered. Someone between you and your connection works as an intermediary, listening in on your communications and possibly **modifying** them.
4. Denial of Service: This prevents the normal use or management of communication facilities. One form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade the performance. It is like shutting down a **server** that could not otherwise be compromised.
It is quite difficult to prevent active attacks absolutely, as this would require physical protection of all communications facilities and paths at all times. Instead, the goal is to detect them and to recover from any disruption or delays caused by them.

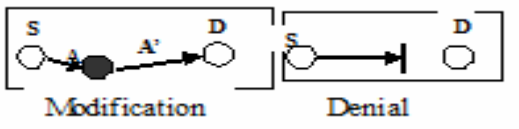


Figure 2: Types of Active Attacks

Figure 2 represents type of Active attacks, S represents Source and D represents Destination.

III. RELATED WORK

Despite the fact that security of Ad Hoc routing protocols is causing a major roadblock in commercial application of this technology, only a limited work has been done in this area. Such efforts have mostly concentrated on the aspect of data forwarding, disregarding the aspect of topology discovery. On the other hand, solutions that target route discovery have been based on approaches for fixed-infrastructure networks, defying the particular ad hoc network challenges. Dahill et al. proposed ARAN[3], It assumes managed-open environment, where there is a possibility for pre-deployment of infrastructure. It consists of two distinct stages. The first stage is the certification and end-to-end authentication stage. Here the source gets a certificate from the trusted certification server, and then using this certificate, signs the request packet. Each intermediate node in turn signs the request with its certificate. The destination then verifies each of the certificates, thus the source gets authenticated and so do the intermediate nodes. The destination node then sends the reply along the route reverse to the one in the request, reply signed using the certificate of the destination. The second stage is a non-mandatory stage used to discover the shortest path to the destination, but this stage is computationally expensive. It is prone to reply attacks using error messages unless the nodes have time synchronization. Papadimitratos and Haas [11] proposed a protocol (SRP) that can be applied to several existing routing protocols. This protocol assumes a security association between source and destination nodes. Intermediate nodes do not need to cryptographically validate the control traffic. It adds a SRP header to the base routing protocol (DSR or AODV) request packet. SRP header has three important fields—QSEQ which helps prevent replay of old outdated requests, QID and random number which helps prevent fabrication of requests, and a SRP MAC which ensures integrity of the packets in transit. SRP requires that, for every route discovery, source and destination must have a security association between them. Furthermore, the paper does not even mention route error messages. Therefore, they are not protected, and any malicious node can just forge error messages with other nodes as source. ARIADNE [18], is based on DSR [5] and TESLA [1] (on which it is based its authentication mechanism). ARIADNE prevents attackers/compromised nodes from disrupting uncompromised routes comprising of benign nodes. It uses highly efficient symmetric key cryptography. ARIADNE does not guard against passive attackers eavesdropping on the network traffic. It does not prevent an attacker from inserting data packets. ARIADNE is vulnerable to active-1-1 attacker that lies along the discovered route, who does not forward packets and does not

generate ERROR if it encounters a broken link. It also requires clock synchronization, which we consider to be an unrealistic requirement for ad hoc networks. Perlman proposed a link state routing protocol [14] that achieves Byzantine Robustness. Although the protocol is highly robust, it requires a very high overhead associated with public key encryption. In their paper on securing ad hoc networks [7], Zhou and Haas primarily discussed key management. They devote a section to secure routing, but essentially conclude that "nodes can protect routing information in the same way they protect data traffic". They also observe that denial-of-service attacks against routing will be treated as damage and routed around. Some work has been done to secure ad hoc networks by using misbehavior detection schemes [15]. This approach has two main problems: first, it is quite likely that it will be not feasible to detect several kinds of misbehaving; and second has no real means to guarantee the integrity and authentication of the routing messages.

Looking at the work that has been done in this area previously, it seems that the security needs for ad hoc networks has not been yet satisfied. Also, Ad hoc networks services are provisional and batteries are a limited resource.

IV. SECURITY MODEL

Most previous work on secure ad hoc network routing relies on asymmetric cryptography such as digital signatures [7, 17]. However, computing such signatures on resource-constrained nodes is expensive, and it is assumed that nodes in the ad hoc network may be so constrained. As a general design principle, a node trusts only itself for acquiring information about which nodes in the network are malicious. In general, ad hoc network routing protocols do not need secrecy or confidentiality. These properties are required to achieve privacy or anonymity for the sender of messages. The proposed scheme has taken into account the following design criteria as to achieve complete security in terms of availability, integrity and authentication, minimal overhead, network performance in terms of throughput and node mobility.

The proposed scheme is based on the hash key chain mechanism. Hash key chains are constructed by using only symmetric cryptographic primitives, namely hash functions. Authentication and integrity can be achieved by using hash key chains. A hash key chain is configured as a recursive chain, where the node first chooses a random key, K1. Subsequent keys are calculated by calculating the one-way hash over the key:

$K_2 = H [K_1]$, $K_{N-2} = H [K_{N-1}]$, $K_{N-1}. = [K_N]$ ….

To compute any previous key from key K_I where $J < I$ a node uses the equation: $K_j = H_{I-J} [K_I]$.

This equation is used by any node to authenticate any received value on the hash chain. If the computed value matches previous known authentic key value then the received key is authentic. Each node discloses each key of its one-way key chain in a particular order, which is exactly reverse of the order in which the keys were generated. The key disclosure schedule and key generation schedule should be reverse For example if the keys were generated by a node in the order K_N ; K_{N-1}; …..K_1; K_0 then the node discloses them in the order K_0; K_1; …. K_N. The rationale behind having the key disclosure schedule to be reverse of the key generation schedule is that K_N of a node is known to all other nodes and in such a situation they should be able to authenticate any subsequent keys that are disclosed. The use of one way hash function allows K_0; K_1; …. K_{N-1} to be authenticated using K_N but K_N cannot be authenticated using any other key value. Hence the key disclosure schedule and key generation schedule is reverse. The scheme was proposed earlier by Leslie Lamport [6]. Hashing is done for route request, reply and local route repair and not in route error and route erasure phases so that less overhead occurs. If in REQ phase if intermediate node cannot satisfy the security requirements, the REQ packet is dropped and not forwarded. Some mobile nodes will be compromised during the operation. Arrival of REQ to Destination will ensure a safe path. REP packet contains this security information specified by sender. So an additional field is added to REQ and REP packet formats. This scheme will be able to take care of external attacks. In order to check internal attacks, some of the techniques that can be used are: Flooding of packets for false route requests, false route replies and also using one way hash to achieve objectives of tampering can be done to take care of internal attacks. As is evident from proposed scheme, the format size will be increased with inclusion of Hash key generation. The routing load will increase due to incorporation of security. It is also clear that the scheme affects the packet delivery fraction and end-to-end delay. The packet delivery fraction will be marginally reduced. Also chances of packets drop may increase due to delay produced in route reply case. This could be improved by having higher timeouts for packets buffered for route discovery.

V PROPOSED SCHEME

The proposed scheme takes care of on demand routing and also power features along with the concept of virtual nodes and security parameter. Virtual nodes (VN) are nodes at the one hop distance from its neighbor. These virtual nodes help in reconstruction phase in fast selection of new routes. Selection of virtual nodes is made upon availability of nodes with their power status and security parameter. Each route table has an entry for its power status (which is measured in terms of Critical, Danger and Active state) and number of virtual nodes attached to it with its security parameter. Whenever need for a new route arises, check for virtual nodes are made, their power status is checked and a route is established. Same process is repeated in route repair phase. Route tables are updated at each Hello interval as in AODV with added entries for power status, security and virtual nodes.

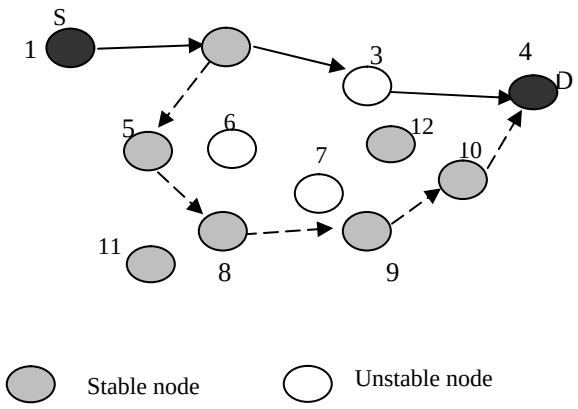


Figure 3: An Example

The proposed scheme is explained with the help of an example shown in Figure 3. It is assumed that there are 12 nodes and nodes are numbered 1 through 12. Assume further that the node with index 1 is the source while destination is the node with index 4. Note that the route discovered using power aware virtual node ad hoc routing protocol may not necessarily be the shortest route between a source destination pair. If the node with index 3 is having power status in critical or danger zone, then though the shortest path is 1—2—3—4 but the more stable path 1—2—5—8—9—10—4 in terms of active power status is chosen. This may lead to slight delay but improves overall efficiency of the protocol by sending more packets without link break than the state when some node is unable to process route due to inadequate battery power. The process also helps when some intermediate node moves out of the range and link break occurs in that case virtual nodes take care of the process and the route is established again without much overhead. In Figure 1 if the node with index 8 moves out, the new established route will be 1—2—5—11—9—10—4. Here the node with index 11 is acting as virtual node (VN) for the node with index 5 and the node with index 8. Similarly the node with index 12 can be VN for the nodes with index 7, 10 and 4.

Some work already have been done on using multiple routes approach in ad hoc network protocols; the scheme by Nasipuri and Das [9], Temporally-Ordered Routing Algorithm (TORA) [1], Dynamic Source Routing [18] and Routing On-demand Acyclic Multi path (ROAM) [17], but these algorithms require additional control message to construct and maintain alternate routes. More recent developments are based on Direction Forward Routing (DFR) [17]. When an update is received, a node records the "geographical direction" to where the update came from. When "predecessor" forwarding fails, the packet is forwarded to the "most promising" neighbor in the recorded direction. It is good for denser mediums only. Another change is Admission Control enabled On demand Routing (ACOR) [10]. Without maintaining up-to- date any routing information and exchanging any routing table periodically, or introducing out weighting signalling functions, a route with QoS requirements is created on-demand.
The proposed routing scheme is designed for mobile ad hoc networks with large number of nodes. It can handle low, moderate, and relatively high mobility rates. It can handle a variety of data traffic levels. This scheme has been designed for use in networks in which all the nodes can trust each other, and there are no malicious intruder nodes. There are three main phases in this protocol: RREQ (Route Request) phase, REP (Route Reply) phase and ERR (Route Errors) phase. The message types are also defined by the protocol scheme.

A. Route *Construction* (RREQ) Phase

This scheme can be incorporated with reactive routing protocols that build routes on demand via a query and reply procedure. The algorithm works by sending a RREQ (route request) propagation process when a source needs to initiate a data session to a destination but does not have any route information; it searches a route by flooding a ROUTE REQUEST (RREQ) packet. RREQ packets have an additional field called SECUR that indicates the required security parameter for the route the sender wishes to discover. This field is only set once by the sender and does not change during the route discovery phase. When an intermediate node receives a RREQ packet, the protocol first checks if the node can satisfy the security requirement indicated in the packet. If the node is secure/capable enough to participate in the routing, The proposed NEW scheme behaves like AODV and the RREQ packet is forwarded to its neighbours. If the intermediate node cannot satisfy the security requirement, the RREQ packet is dropped and not forwarded. The arrival of a RREQ packet at the destination indicates the presence of a path from the sender to the receiver that satisfies the security requirement specified by the sender. The destination node sends the RREP packet as in AODV, but with additional information indicating the maximum security available over the path.
Each RREQ packet has a unique identifier so that nodes can detect and drop duplicate packets. An Intermediate node with an *active route* (in terms of power and Virtual Nodes), upon receiving a no duplicate RREQ, records the previous hop and the source node information in its route table. It then broadcasts the packet or sends back a ROUTE REPLY (REP) packet to the source if it has an *active route* to the destination. The destination node sends a REP via the selected route

B. *Route Error and Maintenance (REP) Phase*

Data packets are delivered through the primary route unless there is a route disconnection. When a node detects a link break (e.g. Figure 4, receives a link layer feedback signal from the MAC protocol, the node with index 1 does not receive passive acknowledgments, the node with index 2 does not receive hello packets for a certain period of time, etc.), it performs a one hop data broadcast to its immediate neighbors. The node specifies in the data header that the link is disconnected and thus the packet is candidate for alternate routing. Upon receiving this packet, previous one hop neighbor starts route maintenance phase and constructs an alternate route through virtual nodes by checking their stability and power status.

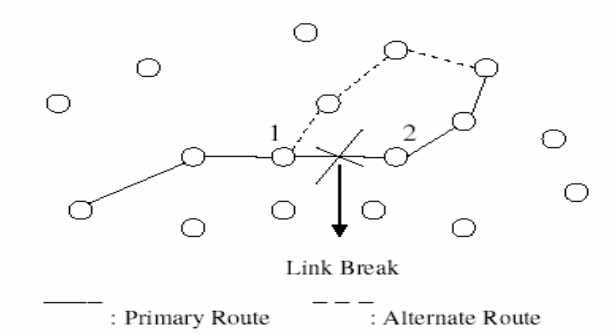


Figure 4: Pictorial Form of Route Error and Maintenance Phase

Nodes which have an entry for the destination in their alternate route table transmit the packet to their next hop node. Data packets, therefore, can be delivered through one or more alternate routes and are not dropped when route breaks occur. To prevent packets from tracing a loop, these mesh nodes forward the data packet only if the packet is not received from their next hop to the destination and is not a duplicate. When a node of the primary route receives the data packet from alternate routes, it operates normally and forwards the packet to its next hop as the packet is not a duplicate. The node that detected the link break also sends a ROUTE ERROR (ERR) packet to its previous neighbor to initiate a route rediscovery. The reason for reconstructing a new route instead of continuously using the alternate paths is to build a fresh and optimal route that reflects the current network topology. Figure 3 shows the alternate path mechanisms at the time of route error ERR. In this phase when route error message sent to previous neighbor of any intermediate node it just reinitiate route construction phase by considering power status of all its virtual nodes. All this route maintenance occurs under *local repair* scheme.

Local Repair

When a link break in an active route occurs, the node upstream of that break may choose to repair the link locally if the destination was no farther and there exists VNs that are active. To repair the link break, the node increments the sequence number for the destination and then broadcasts a REQ for that destination. The Time to live (TTL) of the REQ should initially be set to the following value

TTL = max (VN attached, 0.5 * #hops) + POWER status,

where #hops is the number of hops to the sender (originator) of the currently undeliverable packet. Power status is checked from route table, VN attached is the number of virtual nodes attached.

This factor is transmitted to all nodes to select best available path with maximum power. Thus, local repair attempts will often be invisible to the originating node.The node initiating the repair then waits for the discovery period to receive reply message in response to that request REQ. During local repair data packets will be buffered at local originator. If, at the end of the discovery period, the repairing node has not received a reply message REP it proceeds in by transmitting a route error ERR to the originating node. On the other hand, if the node receives one or more route reply REPs during the discovery period, it first compares the hop count of the new route with the value in the hop count field of the invalid route table entry for that destination. If the hop count of the newly determined route to the destination is greater than the hop count of the previously known route the node should issue a route error ERR message for the destination, with the 'N' bit set. Then it updates its Route table entry for that Destination. A node that receives a ERR bit set. Then it updates its Route table entry for that Destination. A node that receives a ERR message with the 'N' flag set must not delete the route to that destination. The only action taken should be the retransmission of the message. Local repair of link breaks in routes sometimes results in increased path lengths to those destinations. Repairing the link locally is likely to increase the number of data packets that are able to be delivered to the destinations, since data packets will not be dropped as the ERR travels to the originating node. Sending a ERR to the originating node after locally repairing the link break may allow the originator to find a fresh route to the destination that is better, based on current node positions. However, it does not require the originating node to rebuild the route, as the originator may be done, or nearly done, with the data session. When a link breaks along an active route, there are often multiple destinations that become unreachable. The node that is upstream of the lost link tries an immediate local repair for only the one destination towards which the data packet was traveling. Other routes using the same link must be marked as invalid, but the node handling the local repair may flag each newly lost route as locally repairable; this local repair flag in the route table must be reset when the route times out. In AODV, a route is timed out when it is not used and updated for certain duration of time. The proposed scheme uses the same technique for timing out alternate routes. Nodes that provide alternate paths overhear data packets and if the packet was transmitted by the next hop to the destination as indicated in their alternate route table, they update the path. If an alternate route is not updated during the timeout interval, the node removes the path from the table. Figure 4 represents block diagram for route recovery phase.

C. *Route Erasure (RE) phase*

When a discovered route is no longer desired, a route erasure broadcast will be initiated by Source, so that all nodes will update their routing table entries. Figure 5 represent a view of route erasure procedure. A full broadcast is needed because some nodes may have changed during route reconstruction. RE can only be invoked by SRC (source).
The ERR message is sent whenever a link break causes one or more destinations to become unreachable from some of the node's neighbors.

External attacks in PAVNR

1. Routing table inconsistencies**:** A malicious node impersonates another node and sends routing updates. False route requests, replies and updates could cause inconsistencies in the routing table.
2. Wrong routing**:** Tampering of control messages, which could result in incorrect route information.
3. Denial of Service**:** This can be done generating false broadcast packets like route requests. The network can be flooded with wasteful packets thereby preventing channel access to rightful users.

Internal Attacks in PAVNR

1. Generation of false messages: This could be done by generation of false control messages like route requests. It is extremely difficult to differentiate between a misbehaving node and a node that genuinely needs to establish routes to many other nodes.
2. Data tampering: A compromised node could tamper with information and cause havoc in the network.
3. Not forwarding packets: Not forwarding data/control packets could cause considerable damage.
4. Sending false replies: An intermediate node that does not have a route to the destination can falsely reply, thereby causing discovery of wrong routes.
5. Forwarding packets to incorrect nodes: If a packet is forwarded to an incorrect node, the packet may either never reach the destination or the path it takes might be a very costly one.

VI SIMULATION STUDY

Simulation study has been carried out to study the performance study of proposed protocol. Simulation Environment used for this study is NS 2.26 [9]. Some of important parameters are:

A. Degree of Connectivity among Nodes

In many scenarios simulated in previous simulation studies of ad hoc networks, nodes were usually densely connected. In a highly dense network, almost every node has at least a path to any other node, usually just a few hops away. Meanwhile due to the high volume of routing control messages, congestion happens frequently in such networks. A sparsely connected ad hoc network bears different characteristics. In such a network, paths between two nodes do not always exist, and routing choices are more obviously affected by the mobility of the network. In the simulation study, simulations have been carried out in both sparse and dense networks. Area of simulation for dense medium selected has been taken as 1km*1km, and the number of nodes to be 20 and 50. The transmission range of each node in the dense network is 300 m. In case of sparse medium the nodes have been taken as 10 and network area as 700*700 meters whereas the range of transmission is 200 m.

B. Degree of Mobility

Varying the degree of mobility, or the moving speed of each node in the network, is a useful way to test how adjustable a routing protocol is to the dynamic environment. There is several mobility models used in the past. The proposed scheme uses the random waypoint because this has been used more widely than other mobility models. In this model, each node begins the simulation by remaining stationary for a fixed “pause time” seconds. It then selects a random destination in the simulation space and moves to that destination at a speed distributed uniformly between a minimum and a maximum speed. Upon reaching the destination, the node pauses again for “pause time” seconds, selects another destination, and proceeds there as previously described, repeating this behaviour for the duration of the simulation. In the simulation scenes, the minimum moving speed has been taken as 0 and maximum speed as 20m/sec. Different speeds as 1, 2, 5, 10, 15 and 20 meters per second have been used for checking effect of mobility. The pause time has been varied between 0 to 600 seconds. A pause time of 0 second corresponds to continuous motion, and a pause time of 600 corresponds to no motion.

C. Number and Duration of Data Flows

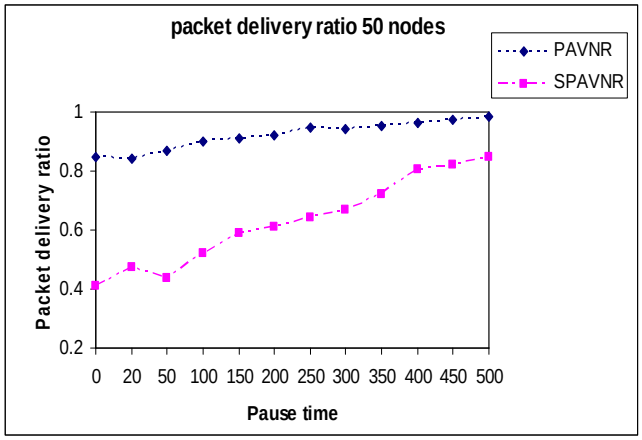
Because on-demand protocols query routes only when data flows exist for them, the number of data flows would influence the number of paths found and the control overhead for on demand protocols, such as AODV, TORA and DSR. How well a protocol adjusts to the change of data flows is another important criterion for evaluating a routing protocol. In the simulations environment, the number of data flows has been varied between 5 and 50. Many connections have been established among nodes. Distant connections have been set even if connection fails after some time. Random scenarios has been created, where many connecting paths are initially far away and also some initially connected paths move too far away till the end of simulation In most previous simulation studies, each data flow started at an early time of the simulation period, and continued until almost the end of the period. In present simulations, besides this long lasting flow pattern, protocols have been tested under data flows that last shorter time periods. Packet size used is 512 bytes.

D. Other Factors

There have been other factors also for which the scheme has not changed the values and studied the effects. The effect of having a static node or a few static nodes as points of attachments to the Internet, such that most of the traffic in the ad hoc network is to and from such point(s) has not been taken into account. In the simulation environment of the study and several previous simulations, traffic type chosen has been the constant bit rate source (CBR). In a real case, there are all kinds of popular applications with different traffic patterns from CBR. Simulations have been carried out for TCP and UDP both. The behavior of DSR protocol has been quite different for UDP and TCP Packets. DSR handles UDP much nicely compared to TCP packets at fast speeds. To observe the protocols more objectively, it would be worth trying different applications in the future.

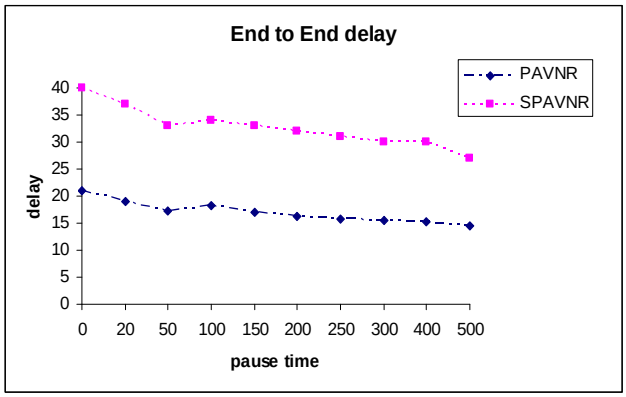
Simulation Results

Graph 1 show the packet delivery ratio based on pause time. The packet delivery ratio is the fraction of successfully received packets, which survive while finding their destination. This performance measure determines the completeness and correctness of the routing protocol. Pause time of 0 means very fast moving nodes and 500 shows minimum movement.



Graph 1: PDF using pause time

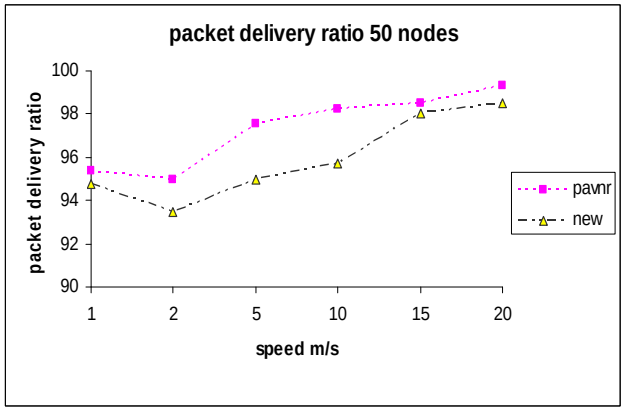
As the graph indicates secured PAVNR has less number of packets delivered, but this reduction in delivery is due to Hash keys calculations and evaluations. Graph 2 represents the end to end delay with respect to pause time. Average end-to-end delay is the delay experienced by the successfully delivered packets in reaching their destinations. This is a good metric for comparing protocols and denotes how efficient the underlying routing protocol is, because delay primarily depends on optimality of path chosen. More end to end delay is observed in this case for secured PAVNR. The reason is again the more calculation part involved for hash key estimation. It should be noted here that only trusted packets are delivered, so some packets does fall because of this reason also.



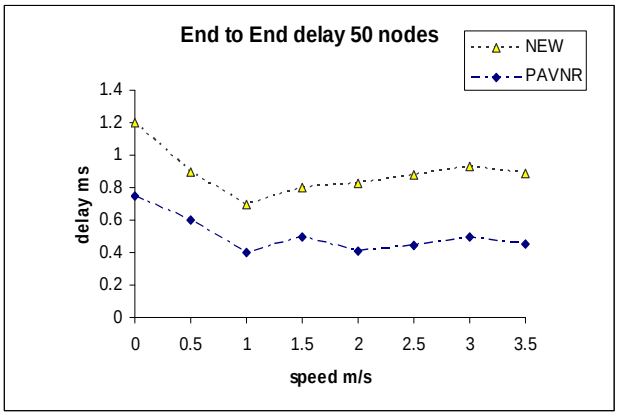
Graph 2: End delay using pause time

The reduction in packet delivery ratio and increase in end to end delay does not show the effectiveness of the proposed scheme. This change will be obvious as more packets are sacrificed to keep them secured. Security is achieved at the cost of performance. Efforts are on to reduce the margins by reducing the size of Hash key.

The experiment has been repeated using speed as parameter in place of pause time. Different speeds have been taken from 1m/s to 20 m/s. The results are shown in Graph 3 for packet delivery ratio and in Graph 4 for end to end delay. Packet delivery is always better for PAVNR than New proposed scheme but New scheme gives more stable and secured routes and it does cause more delays. This delay is in terms of more calculations involved in initial route selection and route table updations. The reduction in packet delivery ratio and increase in end to end delay does not show the effectiveness of the proposed scheme. This change will be obvious as more packets are sacrificed to keep them secured. Security is achieved at the cost of performance. Efforts are on to reduce the margins by reducing the size of Hash key.



Graph 3: PDF using speed as function



Graph 4: End Delay using speed as function

VII. CONCLUSION

An analytical study has been done for contemporary secured routing protocols for Ad Hoc networks. Areas have been identified where further work can be done. A new solution has been proposed as hash key generation. It is clear that different protocols will have different solutions, and it is further suggested that the approach can be utilized in DSR also. The idea has been conceptualized in [18] for DSR. Hash Key management is one of the best options, though other options can also be considered depending upon need of security. As hash key chain is configured as a recursive chain so these keys are noted in route table. This increases memory requirements but hash key management is efficient as it does not involve any additional packet overhead. Important function is that the routing protocol functions very similar to the existing one when there are no external attacks. Whenever an attack occurs additional packets need to be sent to change the routes established by the malicious control packets. This increased traffic size will have its impact on overhead. The overhead is bound to increase with it, but keeping in view of the better secured routing this will have to be done to achieve desired results. Efforts are on to simulate the proposed scheme with different topologies and trying to compare it with existing secured routing schemes. Proposed scheme is expected to work better in dense environments as selection of path becomes easy in case of failures. The research on MANET security is still in its early

stage. The existing proposals are typically attack-oriented in that they first identify several security threats and then enhance the existing protocol or propose a new protocol to thwart such threats. Because the solutions are designed especially with certain attack models in mind, they work well in the presence of designated attacks but may collapse under unanticipated attacks. Therefore, a more ambitious goal for ad hoc network security is to develop a multifence security solution that is embedded into possibly every component in the network, resulting in in-depth protection that offers multiple lines of defense against many both known and unknown security threats.

REFERENCES

[1] A. Perrig, R. Canetti, D. Song, and D. Tygar, "Efficient and secure source authentication for multicast", In Network and Distributed System Security Symposium (NDSS'01), Feb. 2001.
[2] A. Kush, P. Gupta, A. Pandey, C. J. Hawang, "Power Aware Virtual Node Routing Scheme in Ad Hoc networks", IASTED International Conference on Wireless Networks and emerging Technologies(WNET 2004), Banff, Canada, pp. 698-704, July 2004
[3] B. Dahill, B. N. Levine, E. Royer and C. Shields, "A secure routing protocol for ad hoc networks", Technical Report UM-CS-2001-037, University of Massachusetts, Department of Computer Science, Aug. 2001.
[4] C. Parkins and E. Royer, "Ad Hoc on demand distance vector routing", 2nd IEEE workshop on mobile computing, pages 90-100, 1999
[5] D. B. Johnson et al., "The dynamic source routing protocol for mobile ad hoc networks (DSR)", Internet Draft, MANET working group, Feb 2002.
[6] L. Lamport, "Password Authentication with Insecure Communication", Comm. of ACM, 24 (11), pp. 770-772, Nov. 1981
[7] L. Zhou and Z. J. Haas, "Securing ad hoc networks", IEEE Network Magazine, 13(6):24–30, November/December 1999.
[8] M. G. Zapata, "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing", IETF MANET List, Available at draft-guerrero-manet-saodv-03.txt., March 18, 2005.
[9] NS Notes and Documentation, available at www.isi.edu/vint
[10] N. Kettaf, A. Abouaissa, T. Vuduong and P. Lorenz, "Admission Control enabled On demand Routing (ACOR)" available at draft-kettaf-manet-acor-00.txt, July 2006.
[11] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks", SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), Jan 2002.
[12] R. Hauser, A. Przygienda, and G. Tsudik, "Reducing the cost of security in link state routing", In Symposium on Network and Distributed Systems Security (NDSS '97), pages 93–99, San Diego, California, Feb. 1997. Internet Society.
[13] R. Rivest, A. Shamir, L. Adleman, "A method for obtaining Digital Signatures and Public Key Cryptosystems", Communications of ACM, 21 (2), pp. 120-126, Feb. 1978.
[14] R. Perlman, "Fault-tolerant broadcast of routing information", In Computer Networks, n. *7*, pages 395–405, 1983.
[15] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking, pages 255–265, 2000.
[16] T. Karygiannis and L. Owens, "Wireless Network Security", NIST Special Publication 800-48**,** November 2002.
[17] William Stallings, "Cryptography and Network Security: Principles and Practice", pages 3–12. Second edition.
[18] Y. C. Hu, A. Perrig and D. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks", Technical Report TR01-383, Rice University, Dec. 2001.
[19] Yonguang Zhang and Wenke Lee, "Intrusion detection in wireless ad-hoc networks", In 6th International Conference on Mobile Computing and Networking(MOBICOM'00), pp. 275– 283, Aug 2000.
[20] Y. Z. LEE, M. GERLA, J. CHEN, B. Z. A. CARUSO, DFR ("Direction" Forward Routing)" Ad Hoc & Sensor Wireless Networks, Volume 2, Number 2, 2006. pp 01-18.