ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 1, January 2013

A Survey of Performance based Secure Routing Protocols in MANET

Hariom Soni
M.Tech Research Scholar
Department of Computer Science & Engineering
Oriental Institute of Science & Technology
Bhopal (M.P.), India
hariomsoni1988@gmail.com

Asst. Prof. Preeti Verma
Department of Computer Science & Engineering
Oriental Institute of Science & Technology
Bhopal (M.P.), India
preetiverma@oriental.ac.in

Abstract-
An ad-hoc network is a multi-hop wireless network where all nodes cooperatively maintain network connectivity without a centralized infrastructure. If these nodes change their positions dynamically, it is called a mobile ad-hoc network (MANET). Since the network topology changes frequently, efficient adaptive routing protocols such as AODV, DSR, and TORA are used. As the network is wireless, security becomes the major issue in Mobile Ad hoc Networks. Some of the attacks such as modification, fabrication, impersonation and denial of service attacks are due to misbehavior of malicious nodes, which disrupts the transmission. To avoid such attacks some of cryptographic algorithms and key management schemes and some existing security protocols are used. In this paper we represent a survey of performance based secure routing techniques in MANET. The security techniques are categorized based upon different approaches. The security type is borrowed from intrusion detection as either misuse detection or anomaly detection. This paper provides the major improvement in the secure techniques in MANET research using these approaches the features and categories in the surveyed work.

Keywords: ***MANET, Routing Protocol, Security.***

INTRODUCTION

All communications in MANETs take place over the wireless medium. The wireless channels are open, shared and with relatively less power. First, due to the "open" nature of wireless medium, the wireless communication in MANETs is susceptible to eavesdropping that may lead to critical information leakage. The requirement of promiscuous mode raised by many MANET protocols, i.e. continuous monitoring of the shared medium, further facilitates the practicality of eavesdropping. Additionally, wireless transmissions can be intercepted. Once capturing ongoing transmission, adversaries with sufficient knowledge of MANET protocols can meaningfully perform various malicious behaviors. Some typical examples are: alter key information in packets, discard and/or forge messages, inject malicious messages, generate floods of spurious messages, and replay control and data traffic. Such misbehaviors have severe impact on MANETs. For example, MANET routing process requires all nodes dutifully participate in forwarding packets and provide valid routing information. Adversaries who perform either of above malicious behaviors' can ruin the routing functionality [1] and [3].

By supportive infrastructure, we mean entities (or authorities) that perform administrative and management functionalities in MANETs. In a pure at MANET, there is no particular node that is designated as a central authority to execute administrative and management functionalities. Instead, all network operations, including security related control, are on the self-configuration base and in a decentralized way. Whether the security control (e.g., authentication and authorization) or not can be achieved heavily relies on the cooperation of network nodes. However, in the fully distributed and open environment of ad hoc networking, nodes trustworthy are fairly difficult to identify. This provides possible opportunities for misbehaving nodes to harm the security control operation. Meanwhile, the absence of administrative or domain boundaries make the enforcement of any security measures an even more complex problem. In this paper we discussed a survey of performance based secure routing protocol techniques in MANET.

BACKGROUND TECHNIQUES

MANET Security

The theory and experiences have indicated that, due to its unique characteristics, MANETs are suffering from a wide range of security threats and attacks, not only the same attacks their infrastructure counterparts

are facing, but also new ones particularly targeting MANETs.

- ***Unsecured Wireless Channel***

All communications in MANETs take place over the wireless medium. The wireless channels are open, shared and with relatively less power. First, due to the "open" nature of wireless medium, the wireless communication in MANETs is susceptible to eavesdropping that may lead to critical information leakage. The requirement of promiscuous mode raised by many MANET protocols, i.e. continuous monitoring of the shared medium, further facilitates the practicality of eavesdropping. Additionally, wireless transmissions can be intercepted. Once capturing ongoing transmission, adversaries with sufficient knowledge of MANET protocols can meaningfully perform various malicious behaviors. Some typical examples are: alter key information in packets, discard and/or forge messages, inject malicious messages, generate floods of spurious messages, and replay control and data traffic. Such misbehaviors have severe impact on MANETs. For example, MANET routing process requires all nodes dutifully participate in forwarding packets and provide valid routing information. Adversaries who perform either of above malicious behaviors can ruin the routing functionality [1] and [2].

- ***Dynamic Mobility***

In MANETs, freely roaming nodes join and leave the network independently, possibly frequently, and without notice. This dynamic mobility raises several challenges. First, the network topology is constantly changing. More importantly, the mobility makes it difficult in most cases to have a clear picture of the membership. Trust relationship among mobile nodes cannot be assumed to be held in all time, which may lead security solutions with static configuration not to produce expected results. Secondly, the network mobility also makes it difficult to classify nodes as internal nodes or external nodes, which can be easily achieved in traditional infrastructure networks. The classification of internal and external nodes (that is, nodes that belong to the network or not) is important for establishing a line of defense, such as authentication and authorization. Assisted by the absence of trust relationship and classification facilities, adversaries can easily infiltrate MANETs and launch various attacks from inside.

- ***Absence of Central Supportive Infrastructure***

By supportive infrastructure, we mean entities (or authorities) that perform administrative and management functionalities in MANETs. In a pure at MANET, there is no particular node that is designated as a central authority to execute administrative and management functionalities. Instead, all network operations, including security related control, are on the self-configuration base and in a decentralized way. Whether the security control (e.g., authentication and authorization) or not can be achieved heavily relies on the cooperation of network nodes. However, in the fully distributed and open environment of ad hoc networking, nodes trustworthy are fairly difficult to identify. This provides possible opportunities for misbehaving nodes to harm the security control operation. Meanwhile, the absence of administrative or domain boundaries make the enforcement of any security measures an even more complex problem. For example, because mobile nodes move through different network areas and become associated with different do mains, it may be difficult to establish the trust associations of nodes. In turn, MANETs may lack the ground for the establishment of some type of a secret (or keys), so that cryptographic mechanisms can be employed [4] and [6].

- ***Limited Resources***

In order to be light and portable, mobile wireless devices in MANETs cannot be equipped with many resources, such as memory, battery and CPU capacity. The lack of sufficient resources could result in several security risks. First of all, limited computational capabilities of mobile nodes cannot support complicated cryptographic operations, especially if they have to be performed for each packet and over each link of the traversed path. Secondly, mobile nodes have less physical protection, and there-fore are easily stolen, captured and compromised. In many cases, adversaries exploit the compromised nodes to launch the attack. In addition, node's transmission power is typically limited. An adversary with sufficient transmission power and knowledge of the physical and medium access control (MAC) layer mechanisms can obstruct its neighbors from gaining access to the wireless medium.

More importantly, mobile devices could become ideal targets of DoS attacks due to their limited computational capability, memory and battery. An adversary could generate bogus packets, forcing the victim to consume a substantial portion of its resources. Even worse, a malicious node with valid credentials could frequently generate control traffic, such as route queries, at a high rate not only to consume bandwidth, but also to impose cumbersome cryptographic operations on a network node [5] and [7].

Routing Attacks in MANET

Routing protocols (Network layer protocols) extend connectivity from neighboring 1-hops nodes to all other nodes in MANET. The connectivity between mobile hosts over a potentially multi-hop wireless link strongly relies on cooperative reactions among all network nodes. A variety of attacks targeting the network layer have been identified and heavily studied in research papers. By attacking the routing protocols, attackers can absorb network traffic; inject themselves into the path between the source and destination, and thus control the network traffic flow, as shown in Figure 1 (a) and (b), where a malicious node M can inject itself into the routing path between sender S and receiver D.

The traffic packets could be forwarded to a non-optimal path, which could introduce significant delay. In addition, the packets could be forwarded to a nonexistent path and get lost. The attackers can create routing loops, introduce severe network congestion, and channel contention into certain areas. Multiple colluding attackers may even prevent a source node from finding any route to the destination, causing the network to partition, which triggers excessive network control traffic, and further intensifies network congestion and performance degradation.

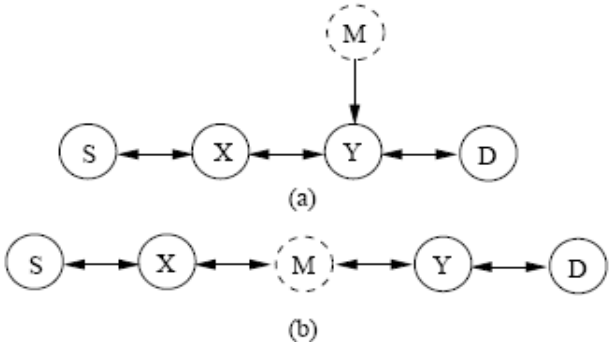

Fig 1 Illustration of Routing Attack

Attacks at the routing discovery phase

There are malicious routing attacks that target the routing discovery or maintenance phase by not following the specifications of the routing protocols. Routing message flooding attacks, such as hello flooding, RREQ flooding, acknowledgement flooding, routing table overflow, routing cache poisoning, and routing loop are simple examples of routing attacks targeting the route discovery phase. Proactive routing algorithms, such as DSDV and OLSR, attempt to discover routing information before it is need, while reactive algorithms, such as DSR and AODV, create routes only when they are needed. Thus, proactive algorithms are more vulnerable to routing table overflow attacks. Some of these attacks are listed below.

- **Routing table overflow attack:** A malicious node advertises routes that go to non-existent nodes to the authorized nodes present in the network. It usually happens in proactive routing algorithms, which update routing information periodically. The attacker tries to create enough routes to prevent new routes from being created.
  The proactive routing algorithms are more vulnerable to table overflow attacks because proactive routing algorithms attempt to discover routing information before it is actually needed. An attacker can simply send excessive route advertisements to overflow the victim's routing table.

- **Routing cache poisoning attack:** In route cache poisoning attacks, attackers take advantage of the promiscuous mode of routing table updating, where a node overhearing any packet may add the routing information contained in that packet header to its own route cache, even if that node is not on the path. Suppose a malicious node M wants to poison routes to node X. M could broadcast spoofed packets with source route to X via M itself; thus, neighboring nodes that overhear the packet may add the route to their route caches.

Attacks at the routing maintenance phase

There are attacks that target the route maintenance phase by broadcasting false control messages, such as link-broken error messages, which cause the invocation of the costly route maintenance or repairing operation. For example, AODV and DSR implement path maintenance procedures to recover broken paths when nodes move. If the destination node or an intermediate node along an active path moves, the upstream node of the broken link broadcasts a route error message to all active upstream neighbors. The node also invalidates the route for this destination in its routing table. Attackers could take advantage of this mechanism to launch attacks by sending false route error messages.

Attacks at data forwarding phase

Some attacks also target data packet forwarding functionality in the network layer. In this scenario the malicious nodes participate cooperatively in the routing protocol routing discovery and maintenance phases, but in the data forwarding phase they do not forward data packets consistently according to the routing table. Malicious nodes simply drop data packets quietly, modify data content, replay, or flood data packets; they can also delay forwarding time-sensitive data packets selectively or inject junk packets.

Wormhole attack: An attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attackers is referred as a wormhole. Wormhole attacks are severe threats to MANET routing protocols. For example, when a wormhole attack is used against an on-demand routing protocol such as DSR or AODV, the attack could prevent the discovery of any routes other than through the wormhole.

Attacks on particular routing protocols

There are attacks that target some particular routing protocols. In DSR, the attacker may modify the source route listed in the RREQ or RREP packets. It can delete a node from the list, switch the order, or append a new node into the list. In AODV, the attacker may advertise a route with a smaller distance metric than the actual distance, or advertise a routing update with a large sequence number and invalidate all routing updates from other nodes [1-3] and [6-8].

SURVEY OF SECURE ROUTING TECHNIQUES

Trust Based Secure Routing in AODV Routing Protocol

A.Menaka Pushpa et. al. introduced a perfect trust model in the network layer, and established secure route between source and destination without any intruders or malicious nodes. In this paper, existing AODV routing protocol has been modified in order to adapt the trust based communication feature. Proposed trust based routing protocol is equally concentrates both in node trust and route trust. In this proposed model, route trust plays an equal role with node trust. Using trust value, secure route can be established in the MANET. Here, network security enhancement is completely performed in the lime light of trust value. In the dynamic environment, node can change its characteristics at any time. After successful participation in the route establishment process, the neighbor may behave like as a malicious node. To avoid this, route trust process (one of the process in the modified protocol) continuously monitor the active routes and calculate the current route trust value or the status of the route. But most of the previous works have been concentrated only in the node trust for establishing communication.

This paper explains three main operations; Node trust calculation, Route trust calculation and Trust based route establishment and route monitoring process. This model requires some adequate changes in the existing source initiated routing protocol, AODV. Modified AODV routing protocol establishes route among nodes based on the trust value.

Node Trust Calculation Process:

Various methods have been proposed for calculating node's trustworthiness. Different trust metrics have been evaluated to identify the trust level of node. Each node has opinion about other node's (neighbor) trustworthiness. Node X has an opinion about trustworthiness of one of its neighbor node Y based on Y's previous and current behaviors.

In this paper, a new data structure Neighbor is introduced in each node of the MANET. All the nodes in such environment already maintain Routing Table. Additionally added Neighbor Table should be maintaining in all the nodes for keep tracks the dynamically changing neighbor list and its corresponding node trust value.

Trust computation involves the process of assigning weights (utility/importance factor) to the events that they can monitor and quantified. Weight assignment process depends on the type of application demanding the trust level. Nodes are dynamically assigning these weights based on their own criteria and circumstances. These weights have a continuous range from 0 to +1 representing the significance of a particular event from unimportant to most important. The trust values for all the events of a node can be combined using individual weights to determine the aggregate trust level for another node.

Route Trust Calculation Process:

Route trust is computed by every node for each route in its routing table. Modified extended Routing supports Route Trust calculation process. Existing Routing Table extended with one more field; Route Trust. In this approach, source node selects the route which is having the highest Route Trust value. Route Trust field of every Routing Table entry is updated at some regular interval. In this method, only one additional field is enough to monitor the route trust worthiness.

The proposed approach is the extension of existing AODV routing protocol for creating secure route for communication. Proposed modifications are in acceptable limit. With this minimum overhead, we can easily eliminate the malicious node as well as they can establish a best trusted route between source and destination. Also it creates a secure communication in this environment without any internal attackers.
Using simulation results, the performance of this protocol is not sufficient justified. In the future, it will be incorporate with other MANET routing protocols [1].

DAAODV: A Secure Ad-hoc Routing Protocol based on Direct Anonymous Attestation

Wenchao Huang, Yan Xiong, Depin Chen et. al. proposed a novel secure routing protocol DAAODV which is based on Ad-hoc On-demand Distance Vector routing (AODV). DAAODV takes full advantage of trusted computing technology, particularly the Direct Anonymous Attestation (DAA) and Property-based Attestation (PBA) protocols. DAAODV is an anonymous protocol without requirement of Trusted Third Party (TTP). Moreover, we propose an efficient signing and verification scheme to overcome the potential DoS attacks triggered by the low efficiency of DAA and PBA. In the simulation, the results show that DAAODV is still efficient in discovering secure routes compared with AODV protocol. In this paper, based on AODV and proposed a novel secure ad hoc routing protocol DAAODV which is anonymous and avoids TTP, and prevents from malicious nodes and selfish nodes. The basic idea is to use Direct Anonymous Attestation (DAA) to accomplish full anonymity in the routing protocol and use issuer instead of TTP, and to use property based attestation (PBA) to guarantee that only nodes whose platform is trusted can join the group. The main challenge of implementing this protocol is the cost of DAA and PBA protocol is a little high, so we choose an efficient DAA protocol and propose a new light-weighted signing and verifying protocol to ease the problem. Experiments proves that it is still very efficient compared with AODV protocol.
DAAODV presents almost a fully protection of routing process and it can be more easily analyzed than other protocols for the hosts that could participate in the routing protocol have to run in an anticipated way. The main extra cost of DAAODV via AODV is the establishment of secure link which uses DAA and PBA protocols. The DAA adopted in this paper is very efficient in DAASign and DAAVerify though not efficient in join protocols. However, hosts have already got the certificate in join protocol before deployed, which means only the cost of DAA Sign and DAA Verify are considered in our protocol. Meanwhile, hosts with the certificate could make DAASign which means the bottleneck TTP is no longer needed in the protocol. Additionally, hello messages should be broadcasted after a few seconds for controlling the CHV, which increases the time interval of establishment of secure link. However, only the processes of establishment cost an extra time, and other messages are handled efficiently for they are encrypted by symmetric keys between hosts.
They presented a secure ad hoc routing protocol which can prevent most attacks including worm-hole attacks, vertex cut attacks, and traffic analysis attacks, and adopt a new efficient signing and verifying scheme preventing DoS attacks.
This protocol doesn't use TTP, and doesn't add much overhead in ns-2 simulation. In future work is to make a fine-grained construction of the routing software, as the design of DAAODV on software level is a little coarse-grained. For example, we should make a concrete scheme of operating the PCRs, and should prove that the DAAODV can avoid attacks at the software level [2].

AODVsec: A Multipath Routing Protocol in Ad-Hoc Networks for Improving Security

Cuirong Wang, Shuxin Cai et. al. proposed a secure routing protocol based on multipath routing technology, namely AODVsec, which divides a data unit into several data pieces and transmits these pieces through different paths. By setting security level on each node, AODVsec limits the maximum number of data pieces an intermediate node can forward. In this way, the malicious node cannot get enough data information for breaking the encryption algorithm. Simulation results show that AODVsec improves security with negligible routing overhead by comparison of the traditional multipath AODV routing protocols.

Design and Implementation of AODVsec:
In AODVsec, each node is set a trust level to limit the maximum data piece number that can be transmitted through. Multiple paths are generated from the source to the destination, and the path information is stored in source node's routing table. Before sending each data unit at the source node, each data unit is split into several pieces. AODVsec assigns a data piece to a safer path selected from the local routing table.
Generating Multiple paths:
1) Reverse path: Different from traditional AODV, AODVsec does not look up from the broadcast list

when generating the reverse path. The routing table's update time should follow the three following principles. To establish connection to the destination node, the source node broadcasts a request PREQ. On the receipt of source's PREQ at the first time, the intermediate node inserts a reverse path to the local broadcast list. When it receives sources PREQ from other path, it stops looking up local broadcast list and adds another reverse path. Only the following three conditions satisfy, update the routing table:

• If there is no route to the source in the routing table, AODVsec adds this new route to the routing table.

• If the number of the routing paths to the source has not hit the maximum number, which should be set according to practical requirements and node number, AODVsec adds this new route to the routing table.

• If there is a route update request which transmits through less hops, even the routing path number hits the maximum limit, AODVsec updates routing table by adding this new routing path.

2) Forward path: In AODV protocol, before sending back the response packet RREP, the node looks up the reverse path existed in the routing table, through which RREP is sent back, and finally the forward path is generated. While in AODVsec, if we query routing table to choose the reverse path based on AODV's mechanism, we will get the same result on every attempt of query. In this way, they generate a single forward path. When a node sends RREP, AODVsec uses the new route query function for choosing the particular reverse path with least sent RREP message. Thus, all the reverse paths would be used as round robin, and multiple forward paths could be established.

Node's Trust Level:

1) Data Fragmentation and Encryption: If malicious node captures an entire data unit, it can do some decryption work to get the original data, which is very insecure for a communication system. To prevent this situation, AODVsec divides each data unit (e.g., a data packet) into several pieces, every piece is encrypted solely. There are many encryption methods; they choose a less complicated XOR Encryption method to cut down the computation cost.

2) Trust Level: Trust level is a mathematical metric to evaluate a node's security. The higher the trust level is, the securer a node is. In AODVsec, the trust level also limits the maximum piece number a intermediate node can forward, which belong to a same data packet unit. In specific, there are 4 pieces that come from a same data packet. An intermediate node with trust level of 3 can forward 3 pieces at most.

First, they compare the access violation ratio between traditional multipath AODV and AODVsec. Due to AODVsec sets trust level for each node, it decreases access violation ratio to a large extent. With the reduction of trust level, the access violation ratio is higher accordingly. For AODVsec does not supply satisfied synchronization when two paths cross, AODVsec cannot ensure each node's access violation ratio as 0. In AODVsec, as most nodes' trust level is high, all data pieces may be sent out before they hit the maximum trust level. Thus, it is no need to reselect routing path, and the routing overhead is relatively low. While traditional multipath AODV uses another path when the transmission path is down, continuously re-selecting path results more routing overhead. When AODVsec running under lower trust level's situation, the routing overhead is bigger. This is because a data packet's all pieces have still not been sent out, all the paths reach the upper limit that results in re-select routing path and more routing overhead. protocol.

The results show that AODVsec outperforms traditional multipath routing on ensuring security. As a common case, attacker cannot intercept all the paths, AODVsec avoids maliciously accessing a entire data packet, so it improves system's security with negligible routing overhead.

The AODVsec still has some imperfect points. As a future work, it will need to focus on designing the synchronization control mechanism to solve this problem [3].

Security subsystem for Ad Hoc Wireless Networks

Zeyad M. Alfawaer and Saleem Al_zoubi et. al. proposed an effective security AODV algorithm called ES-AODV to enhance the data security. Simulation results show that the proposed algorithm provides a reasonably good level of security and performance. The overall goal of this algorithm is to provide a secure solution for communication in ad hoc network applications strong enough to withstand an active internal threat within the network. This protocol will be able to find a trusted end-to-end route free of any malicious entity, effectively isolating any node trying to inject malicious information into the network.

The proposed security routing protocol is based on the following assumptions. Our main focus is on the network layer and the protocol that we propose here is an extension of the Ad hoc On Demand Distance Vector (AODV) routing protocol which we call effective security AODV (ES-AODV). And we assume that all the nodes are identical in their physical characteristics and all communicate via a shared wireless channel and operate in a promiscuous mode. They have assumed a reliable link layer protocol.

This model is based on collaborative effort of all the nodes and analysis of different malicious behavior.

They don't encourage the notion of trust transitivity; this trust transitivity encourages more colluding attack in the network from multiple malicious nodes. Essentially all routing protocols in the ad hoc community tend to find the shortest path to the destination irrespective of the presence of any malicious node in that path. The model against that, emphasize on a path free of malicious node is more important than the shortest path. Designing ES-AODV comes from finding a trusted end-to-end path free of malicious nodes. The basic idea behind the protocol is for a node to append the trust level of its predecessor from which has received the route request packet. Trust levels are defined to be unique values of the level of trustworthiness of a node on another node. A path with maximum trust level will eventually be selected by the destination node and will be sent to the source as the end-to-end active path to be used. A node with malicious intention will try to put itself into that active route by trying to inject malicious trust information.

The protocol will ensure that all the trust level information provided by a node will be checked by its predecessor node in order to ensure information authenticity. This is ensured by computing a signature with the Private Key of the node, along with the trust level computation. When a node wants to find a route to another node, it initiates a route discovery.

They evaluate different scenarios of attack by a malicious entity, acting either independently or in collusion, and show that the protocol is secure against these attacks.

A malicious node wants to include itself into the path and provides wrong information in the RREQ packet - this attack has already been prevented while designing the ES-TAODV protocol. The malicious node is effectively isolated by the collaborative effort of its neighbors. Furthermore, A node falsely accuses another node and alters the information provided by the later - the accuser has to append the signature computed by the accused node. In order to alter the information, it has to decrypt the signature, change the original information and recomputed it. But it fails to recompute the signature as it lacks the knowledge of the accused node's Private Key. Thus any attempt to alter the original information gets detected. In addition, a node whose trust level has changed, falsely accuses another node by using a copy of the old Signature field that the later used at some earlier point of time. This false accusation gets detected as the decryption of the signature will reveal the actual source address and broadcast ID pair. They recognize that the protocol is secure under these threats.

The efficient security algorithm ES-AODV enhances the security in ad hoc wireless networks. According to the analysis of the results obtained from extensive simulation, it concludes that the secure routing solution scales well to both mobility and network size.

The routing protocol performs Does not better than the existing secure AODV routing protocol with increased mobility in the network. It should be improve in future extension [4].

QOS Based Performance Evaluation of Secure On-Demand Routing Protocols for MANET's

Muhammad Naeemv, Zah ir Ahmed , Rashid Mahmood and Muhammad Ajmal Azad et. al. evaluated the two secure routing protocols Ariadne and SAODV in the performance aspects instead of security aspects under Random Way Point and Manhattan Grid mobility models. They

used and implement the extension of AODV that is Secure Adhoc on-Demand Distance Vector routing protocol (SAODV) and the extension of DSR that is Ariadne in the Network Simulator 2

(NS-2). In this paper they compare this protocol on basis of following quality of service parameters like delay, jitter, routing overhead, route acquisition time, throughput, hop count, packet delivery ratio using manhattans grid and random waypoint mobility models. The main aim is to find out the payload a node has to pay to guarantee the good quality of service.

To perform evaluation for the project, they have used the implementation of Ariadne by Monarch Project people. The implementation makes use of TESLA as a broadcast authentication protocol for the efficient key distribution and key management. The implementation demands the use of earlier version of NS-2 i.e. ns-allinone2.1b4a along with the CMU's extensions to the network simulator i.e. emu-extensions. The protocol has been implemented by modifying the original DSR implementation files and doesn't exist as an independent protocol. Using this implementation for simulations requires having three different files i.e. a movement model file, a communication model file and a protocol specific file.

In the results analysis it performed number of simulations to show the effectiveness, usefulness and performance of routing protocols architecture. They have run number of simulations with variable nodes and communication flows in each simulation; a node may have send data to other node or act as an intermediate node. Each simulation runs for 100 second. Route Acquisition Time, Normalized Routing Overhead, Average Hop per Count, Throughput, Jitter and Packet Delivery Ratio, Mean

End-to-End Delay is considered to evaluate the performance of the protocols.

They evaluated two secure routing protocols for the mobile Ad-Hoc networks (MANETs) under the Random Way and Manhattan Mobility Model with the performance metrics despite the security metrics. Ariadne performs better in term of route acquisition time and routing overhead over the SAODV. The routing protocol SAODV takes advantage in term of end-to-end delay and packet delivery fraction over the Ariadne . As they have seen in the graphs the performance has increasing as the number of nodes is increased. The protocol overhead of SAODV is greater as compared to Ariadne. TESLA provides the edge to Ariadne, as TESLA is very lightweight algorithm and SAODV using hash chains and digital signatures demands for extensive computing. Ariadne with the use of TESLA is more protected, reliable and efficient than SAODV as the number of nodes increasing. In conclusion, to route the data packets securely Ad-Hoc routing protocols are essential.

In the implementation of such routing protocols, the need is to eliminate the shortcoming of these protocols by evaluating performance of them on a simulation platform. To minimize the associated overhead like delay, routing overhead demands an intensive optimization in both the protocols. In future it will require more specifically SAODV to decrease the processing requirements to tackle hash chains and digital signatures to implement the security [5].

Agent-Based AODV Routing Protocol in MANET

Preeti Bhati, Rinki Chauhan and R K Rathy et. al. tried to remove the existence of misbehaving nodes that may paralyze or slows down the routing operation in MANET. This increases the efficiency of a network. Efficiency can be calculated by the parameters or factors such as transmission capacity, battery power and scalability. Here they are considering the most crucial factor named as transmission capacity of a node. In MANET, as the network size increases complexity of a network also increases. To overcome this they make network as modular. So the network becomes task specific which refer to a particular work only. This is the reason of infusing the concept of agents in an efficient network. This proposed protocol provides the most efficient and reliable route which may or may not be minimum hop count.

They proposed an innovative Efficient Agent Based Adhoc on-Demand routing protocol (ABAODV) for MANET. The purpose of Efficient AB-AODV selects the most efficient, minimum overhead and may be minimum hop count route from the different possible routes. The mobile agent paradigm has attained the attention from many field of Computer Science in Wireless communication. The proposed scheme uses mobile agent that can move in the adhoc network to discover the network topology and collects or updates the routing table. Also it will evaluate transmission capacity value for each node by a formula discussed later. This would be performing by the fusing of mobile agent at every node which computes routing information. The static agent that runs in a host node supplies they require information to the visiting mobile agent. Therefore the proposed protocol uses a Monitoring Agent System (MAS) and Routing Agent System (RAS) to achieve the required task. *MAS* are responsible for monitoring the host node behavior and activities like calculating transmission capacity value of a node including in the routing process. Efficiency can be achieved by using the transmission capacity value of a node. *RAS* is responsible for using the already calculated transmission capacity information and finding out the most reliable and efficient route for a destination. When a mobile agent wants to find the most efficient path, it moves from one node to another node. Therefore each mobile agent should have a unique *mobile ID* and carries the briefcase which contains all the possible routing information needed during the movement of agent. Also a host node contains the routing cache which is updated by the stationary agent.

The development of their transmission capacity value calculation is based on the Secure and Objective Reputation based Incentive (SORI) basic scheme. In that scheme monitoring of neighbor node is used to collect information about the packet forwarding behavior of all the neighbors. Due to the promiscuous mode they consider, a node may be capable of overhearing the transmissions of its neighbors. Therefore with this capability, a mobile node *N* can maintain a neighbor node list (denoted by *NNLN*) which contains all of its neighbor nodes that node *N* learned by overhearing. Also, node *N* keeps track of two numbers, for each of its neighbor (denoted by *M*), define as below:

• *FNN (M) (Request-for-Forwarding):* The total number of packets that node *N* has transmitted to node *M* for forwarding.

• *FTN (M) (Has-Forwarded):* The total number of packets that have been forwarded by node *M* and noticed by node *N*.

These two numbers are updated by the following rules. When node *N* sends a packet to node *M* for forwarding, the counter *FNN (M)* is increased by one. Then node *N* listens to the wireless channel and check whether node *M* forwards the packet as expected. If node *N* detects that node *M* has forwarded the packet before a preset time-out expires, the counter *FTN (M)* is increased by one. *CN*

(M) is a metric called confidence, used to describe how confident node *N* is for its judgment on the reputation of node *M*. In SORI, *CN (M) = FNN (M)*; that is the more packets transmitted to node *M* for forwarding, the better estimation about how well the neighbor M does forwarding. *CN (M)* is used by mobile agent to take decision in efficient routing.

The infrastructure less and dynamic nature of MANET demands new set of networking analysis in order to provide diverse application in many different scenarios. So, it is possible that some application demands less overhead as well as fast processing with efficient transmission. This paper, presents the protocol being proposed which utilizes the dual cooperative mobile agents and stationary agents for routing in dynamic networks as MANET. Every mobile agent computes the transmission capacity of all the nodes so that Routing Agent System (RAS) can take the efficient reliable decision which routing path is more efficient and reliable. Each node has its own stationary agents but number of mobile agents in the network depends on the network architecture or the protocol used.

The transmission capacity factor into the networking as MANET of the protocol will need to improve in future [6].

CONCLUSION

A MANET (Mobile Ad-hoc Network) is an autonomous collection of mobile users that offers infrastructure-free communication over a shared wireless medium. It is formed spontaneously without any preplanning. Multicasting is a fundamental communication paradigm for group oriented communications such as video conferencing, discussion forums, frequent stock updates, and video on demand, view programs, and advertising. The combination of an ad hoc environment with multicast services induces new challenges towards the security infrastructure in routing protocols. In order to secure multicast communication, security services such as authentication, data integrity, and access control and group confidentiality are required. Among which group confidentiality is the most important service for several applications. These security services can be facilitated if group members share a common secret. During the survey on secure routing protocols in MANET, we conclude some points that can be further explored in the future using advanced secure technique and it will improve the performance of secure MANET to achieve more efficient accuracy in network congestion, reduce the end to end delay time, overhead and throughput.

Surveying different techniques we define the Advantages and Disadvantages of techniques in the table:

Techniques	Advantages/ Merits	Disadvantages /Future Improvement Direction
MANET, AODV, Trusted Networks; Trust Model	The proposed approach is the extension of existing AODV routing protocol for creating secure route for communication. Proposed modifications are in acceptable limit. With this minimum overhead, we can easily eliminate the malicious node as well as they can establish a best trusted route between source and destination.	Using simulation results, the performance of this protocol is not sufficient justified. In the future, it will be incorporate with other MANET routing protocols [1].
DAAODV, Secure Routing Protocol	They presented a secure ad hoc routing protocol which can prevent most attacks including worm-hole attacks, vertex cut attacks, and traffic analysis attacks, and adopt a new efficient signing and verifying scheme preventing DoS attacks.	This protocol doesn't use TTP, and doesn't add much overhead in ns-2 simulation. In future work is to make a fine-grained construction of the routing software, as the design of DAAODV on software level is a little coarse-grained [2].
Multipath Routing, Ad-hoc Networks, AODVsec	The results show that AODVsec outperforms traditional multipath routing on ensuring security. As a common case, attacker cannot intercept all the paths, AODVsec avoids maliciously accessing a entire data packet, so it improves system's security with negligible routing overhead.	The AODVsec still has some imperfect points. As a future work, it will need to focus on designing the synchronization control mechanism to solve this problem [3].

WirelessSsecurity1,; MANE, IEEE 802.11b4	The efficient security algorithm ES-AODV enhances the security in ad hoc wireless networks. According to the analysis of the results obtained from extensive simulation, it concludes that the secure routing solution scales well to both mobility and network size.	The routing protocol performs Does not better than the existing secure AODV routing protocol with increased mobility in the network. It should be improve in future extension [4].
MANET, Routing, Security	In the implementation of such routing protocols, the need is to eliminate the shortcoming of these protocols by evaluating performance of them on a simulation platform. To minimize the associated overhead like delay, routing overhead demands an intensive optimization in both the protocols.	In future it will require more specifically SAODV to decrease the processing requirements to tackle hash chains and digital signatures to implement the security [5].
MANET, Secure AODV	This paper, presents the protocol being proposed which utilizes the dual cooperative mobile agents and stationary agents for routing in dynamic networks as MANET. Every mobile agent computes the transmission capacity of all the nodes so that Routing Agent System (RAS) can take the efficient reliable decision which routing path is more efficient and reliable.	The transmission capacity factor into the networking as MANET of the protocol will need to improve in future [6].

REFERENCES

[1] A.Menaka Pushpa, "Trust Based Secure Routing in AODV Routing Protocol", IEEE 2009.

[2] Wenchao Huang, Yan Xiong, Depin Chen, "DAAODV: A Secure Ad-hoc Routing Protocol based on Direct Anonymous Attestation", 2009 International Conference on Computational Science and Engineering, IEEE 2009, pp. 809-916.

[3] Cuirong Wang, Shuxin Cai, and Rui Li, "AODVsec: A Multipath Routing Protocol in Ad-Hoc Networks for Improving Security", 2009 International Conference on Multimedia Information Networking and Security, IEEE 2009, pp. 401-404.

[4] Zeyad M. Alfawaer and Saleem Al_zoubi, "A proposed Security subsystem for Ad Hoc Wireless Networks", 2009 International Forum on Computer Science-Technology and Applications, IEEE Computer Society 2009, pp. 253-255.

[5] Muhammad Naeemv, Zah ir Ahmed, Rashid Mahmood, and Muhammad Ajmal Azad, "QOS Based Performance Evaluation of Secure On-Demand Routing Protocols for MANET's", 20 1O IEEE, ICWCSC 2010X.

[6] Preeti Bhati, Rinki Chauhan and R K Rathy, "An Efficient Agent-Based AODV Routing Protocol in MANET", International Journal on Computer Science and Engineering (IJCSE), Vol. 3 No. 7 July 2011, pp. 2668-2673.

[7] Ming Yu, Mengchu Zhou, and Wei Su, "A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 1, JANUARY 2009, pp. 449-460.

[8] D. Suganya Devi and Dr. G.Padmavathi, "IMPACT OF MOBILITY FOR QOS BASED SECURE MANET", International journal on applications of graph theory in wireless ad hoc networks and sensor networks, pp. 46-57.