MANETS AND PROTOCOLS

Mamatha CR[1], Pavithra S[2], VanithaG[3]
[1]Assistant Professor, Department of Computer Science and Engineering,
Vemana Institute of Technology, Koramangala, Bangalore, Karnataka, India.
[2,3]Student, Department of Computer Science and Engineering,
Vemana Institute of Technology, Koramangala, Bangalore, Karnataka, India.
[1]mamatha.cr@vemanait.edu.in; [2]pavithra@vemanait.edu.in; [3]vanitha@vemanait.edu.in

Manuscript History
Number: IRJCS/RS/Vol.06/Issue06/JNCS10097
Received: 29, May 2019
Final Correction: 30, May 2019
Final Accepted: 02, June 2019
Published: June 2019
doi://10.26562/IRJCS.2019.JNCS10097
Editor: Dr.A.Arul L.S, Chief Editor, IRJCS, AM Publications, India

Abstract - Multipath Routing Protocol for Mobile Adhoc Networks, Currently data routing based on Qos(Quality of Service) is the most required domain.The mobile adhoc network needs to have lower cost calculation or matric technique,which is mandatory for higher Quality of Service. The technique that helps to modify the quality of the shortest path randomly based on clients QoS requirements and existing traffic load, this type of problems can be solved easily by specifically designing Multi-Protocol Enabled Network. A secure hybrid ad hoc routing protocol, called Secure Zone Routing Protocol (SZRP), it aims at addressing the limitations by combining the best properties of both proactive and reactive approaches. The proposed protocol is based on the concept of zone routing protocol (ZRP). It presents a secure minimized dominating set routing protocol for mobile adhoc network based on delay tolerant network. In the proposed model, the route selection is based on concept of virtual network topology, in that the messages are routed only to trustable nodes in minimized dominating set.

Keywords: Mobile Ad-hoc Networks (MANET), Ad-hoc On-Demand Distance Vector (AODV), Trust model, Secure routing protocol, Ad-hoc networks. ZRP-Zonal Routing Protocol,SZRP-Secure Zonal Routing protocol

I. INTRODUCTION

Wireless Ad-hoc network is created of few to hundred numbers of nodes or device that are connected through a radio frequency (RF) of infrared interface and have a capability of communication with one another by creating connected during a decentralized manner. Some examples of wireless adhoc network is as follows:

1. The network accustomed monitor the atmosphere and observe environmental changes.
2. The network accustomed observe and transmit data for military and defense purpose.
3. Network accustomed sense and monitor vehicular traffic on the road.
4. Network for police investigation sensor for providing security in anywhere.
5. Network for patient monitoring system to transmit information from ambulance to doctor and receive medical recommendation from a distance.

IoT is an expanding network of physical devices that are linked to different types of sensors. The different types of sensors helps in functioning connectivity to the internet, that they are able to exchange data.

Routing Protocols

Routing protocols are outlined as a group of rules by that nodes or router sending the packet of data from source to intended node.

Classification of Routing Protocols:

Routing protocol are classified into three basic groups:

A. Pro active Routing protocols

Proactive routing protocols also can be seen as tabledriven protocols. Table driven means that each node or adevice incessantly updates the table containing routing dataconcerning each alternative node of the network.

B. Reactive Routing protocols

Reactive routing protocols also can be seen as on demand protocols. During this variety of routing algorithmic program, all mobile nodes contain the knowledge of solely active paths to thedestination nodes. If any source terminal needs to send packet of knowledge to its supposed node or terminal, reactive routing can try and settle a route supported the request from the source.

C. Hybrid Routing protocols

Hybrid routing protocols are termed as hybrid becausethis protocol is consolidation of higher than represented two varieties of routing protocol together with alocation identification routing algorithmic program and provides the necessities of each.

Mobile adhoc networks

A mobile ad hoc network (MANET),is a wireless network sometimes called a wireless ad hoc network or a mobile mesh network, comprised of mobile computing devices (nodes) that uses wireless transmission for communication, without the aid of any established infrastructure or centralized administration such as a base station in cellular network or an access point in wireless local area network. The nodes organize themselves arbitrarily and are free to move randomly ; thus, the network's wireless topology may change rapidly and unpredictably. Ad hoc networks consist of mobile nodes which communicate with each other through wireless medium without any fixed infrastructure. Mobile ad hoc network (MANET) do not have any fixed infrastructure and consists of wireless nodes that move dynamically without any boundary limitation. MANET includes technical challenges in the area of routing, security, MAC, QoS, and power efficiency. Routing is MANET is one of the main issue as the network topology changes dynamically. It is necessary to maintain the topology changes by periodically updating the routing table which occupies a large part of network traffic. Flat routing protocols are based on global routing. Routing information is flooded to all nodes in the network. These protocols involves large amount of control packet overhead and their performance degrades with increase in network size and node mobility. To overcome the scalability problem we adapt hierarchical network design. Most commonly used routing protocol are based on the concept of clustering which partition the network into group of clusters. Nodes in same cluster communicate directly, whereas nodes in different clusters communicate through cluster heads. Each cluster head knows information about other cluster heads in the network. Virtual network topology can be formed by connecting all the cluster heads in the network. It simplifies routing tables and lower the amount of routing information that is exchanged.

Depending on how nodes establish and maintain paths, routing protocols for MANET broadly fall into pro-active, reactive, hybrid, location based types. In proactive routing Protocol and every node maintains one or more tables representing the entire topology of the network. These Tables are updated regularly in order to maintain an up-to-date Routing information from each node to every other node. To maintain the up-to-date routing information, topology information needs to be exchanged between the nodes on a regular basis, leading to relatively high overhead on the network. One the other hand, routes will always be available on request. Reactive protocols seek to set up routes on demand. If A node wants to initiate communication with a node to which it has no route, the routing protocol will try to establish such a route. Hybrid routing protocols use distance-vectors for more accurate metrics to determine the best paths to destination networks, and report routing information only when there is a change in the topology of the network. Hybrid routing allows for rapid convergence but requires less processing power as compared to link-state routing.

II. METHODS

Network Model and Assumptions during This work, we build some assumptions and establish the network model of MAOMDV(Mobile AdHoc on Demand Multipath Distance Vector).

Algorithm 1

```
General Procedure of Node N2 in Performing modified
Routing Discovery
Receive an RREQ(S,T) from
If Authenticate (N2, N1)== true then
If Authenticate (N2, S)== true then
If Authenticate (N2, T)== true then
Update opinion $w_{N2/N1,wN2/S,wN2/T}$
Update route table of N2
Re-broadcast RREQ
end if
end if
end if
if Every authentication fails then
Update opinion
Do not forward RREQ
end if
```

Algorithm 2

```
Authenticate Function of Node N2 to Node N1Exchange opinions about N1with all the neighbors of N2
/*Judge the next step using the criteria in Table 1*/
If uncertainty>0.5 then
Request and verify N1's certificate
else if disbelief >0.5 then then
Distrust N1 for an expiry time
else if belief >0.5then
Trust N1and re-broadcast RREQ/RREP
else
/*Do not have much confidence about N1's
Trust worthiness.*/
Request and verify N1's certificate, by default
end if
```

i) Secure Zonal Routing Protocol

A. Protocol overview

The Secure Zone Routing Protocol (SZRP) is based on the concept of Zone Routing Protocol (ZRP). It is a hybrid routing protocol and adds its own Security mechanisms to perform secure routing. The reasons for selecting ZRP as the basis of our protocol are as follows:

i) ZRP is based on the concept of routing zones, a restricted area, and it is more feasible to apply the security mechanisms within a restricted area than in a broader area that of the whole network

(ii) Since the concept of zones separate the communicating nodes in terms of interior (nodes within the zone) and exterior (nodes outside the zone) nodes,certain information like network topology and neighborhood information etc. can be hidden to the exterior nodes, (iii) Incase of a failure, it can be restricted to a zone.

B. Design of Secure Zone Routing Protocol

This section describes in details the architectural design of the proposed protocol as a whole and its individual components in particular.We have assumed the following things for the design and successful deployment of the proposed protocol. The network links are assumed to be bidirectional.The Resources of different ad hoc network nodes may vary greatly, from nodes with very little computational resources, to resource rich nodes equivalent in functionality to high performance workstation.

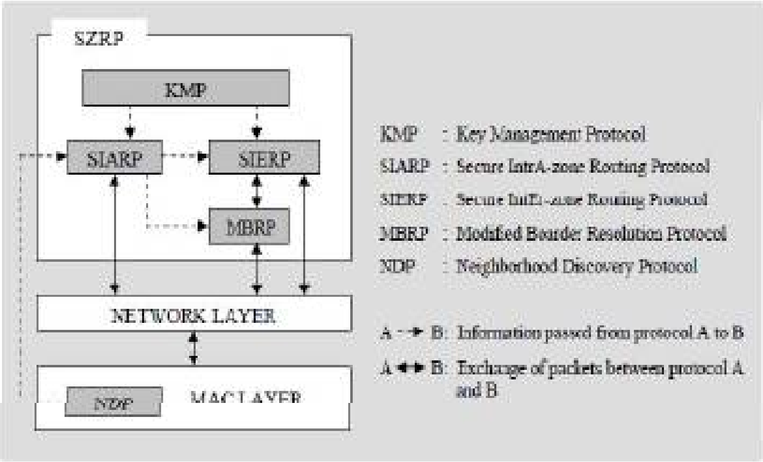
SZRP
KMP
SIARP
SIERP
MBRP
NETWORK LAYER
NDP
MAC LAYER
KMP : Key Management Protocol
SIARP : Secure IntrA-zone Routing Protocol
SIERP : Secure IntEr-zone Routing Protocol
MBRP : Modified Bourder Resolution Protocol
NDP : Neighborhood Discovery Protocol
A - -► B: Information passed from protocol A to B
A ◄► B: Exchange of packets between protocol A and B

Fig.2.1.Architecture of SZRP.

The key management protocol (KMP) is responsible for public key certification process. It fetches the public keys for each CN by certifying them with the nearest CA. The secure intrazone routing protocol (SIARP) and secure inter zone routing protocol (SIERP) uses these keys to perform secure Intra zone and inter zone routing respectively.

C. The Secure Routing Algorithm.

This section describes the secure intrazone and interzone routing in details. We consider the network in Figure 3.2for the illustration. SIARP, at each node, periodicallycomputes the route to all intrazone nodes and maintains this information in SIARP routing table.

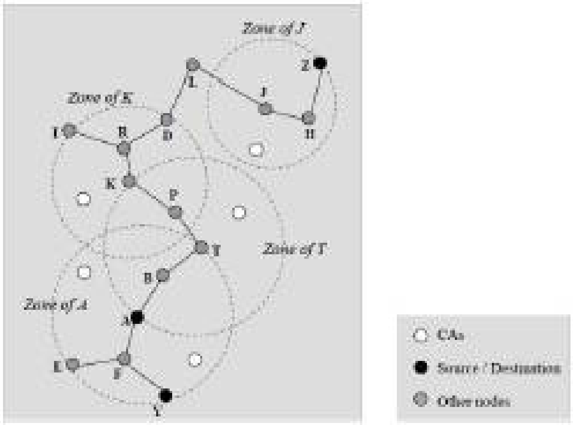

Fig 2.2 IntraZone and InterZone Destinations of Node A

For example in Figure 3.2, node *A*, proactively computes the route to *B*, *T*, *E*, *F* and *Y* and stores this information in its SIARP routing table. This process, called proactive routecomputation. When a node has a data packet for another node, it checks its SIARP routing table to determine whether the destination is within its zone or not. If the destination is within the zone, for example if node *A* has a packet destined for node *Y*, the packet is forwarded to the destination proactively using SIARP. On the other hand if the destination is outside the zone, for example if node *A* wants to transmit a packet to *Z*, then interzone routing is performed using SIERP.

ii) System Model

In this paper, we use the same system architecture as that in reference. Super node system architecture is based on Delay Tolerant Network (DTN) framework. System model consists of heterogeneous wireless networks. Each network is connected to the Internet through DTN gateway. The heterogeneous network includes MANETs. MANET have limited transmission range. Each MANET includes DTN gateway. Gateway is same as mobile node but with extra Power. The architecture is based on centralized modes scheme. But in order to support scalability, the architecture maintains multiple servers, instead of single server in several locations. Severs are referred to as super nodes. Super node can communicate with gateways in the network. Each node during its network connection updates its location details with its super node.

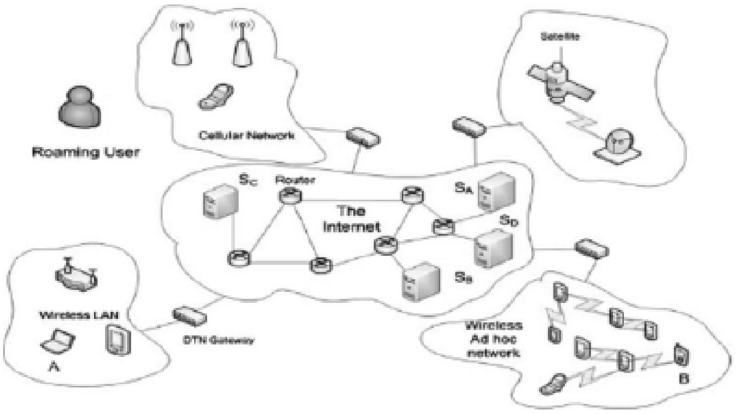

Fig.2.3. The system architecture with super nodes.

A sender before sending message contact its super node to identify the location of destination. Using its super node information sender establish a end to end connection with the destination. If there's any connection failure, the messages are stored in destination's super node. The architecture involves routing in two different levels: routing between super node and gateways; routing between user and gateways. This paper mainly focus on routing between user and gateways.

In this proposed fast and secure protocol, routing is performed through proactive and reactive mechanism. In routers that use dynamic routing protocols, it is important to have fast convergence because routers could make incorrect forwarding decisions until the network has fully converged. In Proactiveprotocol, when a new node is added in the network it takes some time to converge during that time if we want to send data to destination through that new nodeimmediately, it takes some time to converge and then it will transmit the data. To avoid this problem we are going to use reactive protocol instead of proactive in that time that is until network converge. Fig 3.4 shows the architecture model of fast and secure transmit protocol.

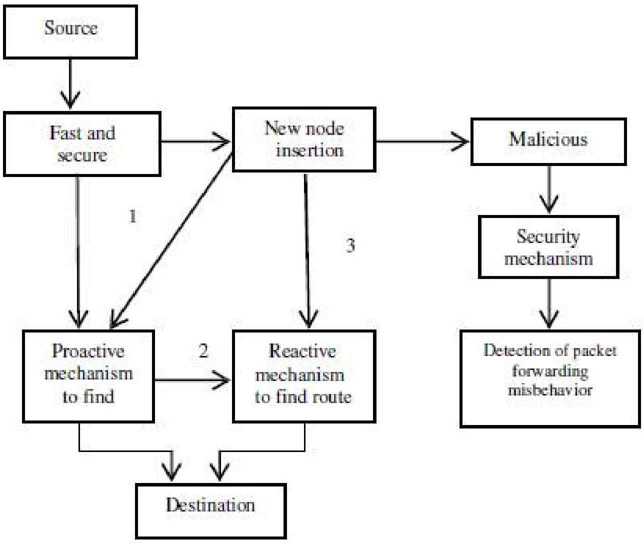
Source
Fast and secure
New node insertion
Malicious
1
3
Security mechanism
Proactive mechanism to find
2
Reactive mechanism to find route
Detection of packet forwarding misbehavior
Destination

Fig.2.4. Architecture of fast and secure transmit protocol.

III. RESULTS

A. Simulation Scenario and Settings We used the NS-2 simulator in version 2.28. The AODV-UU was used in version 0.9.1. to generate results that can be compared to existing results in the literature tried to reuse the scenarios presented by Perkins et al.

1) Physical Model:

For the physical propagation model we used the two-way ground model. In the simulator we applied the parameters of a 2.4 GHz Lucent Orinoco Wave LAN DSSS Radio Interface. The data rate was set to 11 Mb s and a transmission range of 170 m was used.

2) Media Access Model:

For media access we used the commonly known distributed coordination function (DCF) mode of the IEEE 802.11 wireless LAN standard. Combined with the physical model a standard WLAN adapter has been used in the model.

3) Mobility Model:

To simulate node mobility we used the Random Waypoint Mobility model. The model has some drawbacks, however, since we wanted to obtain comparable results to the existing results we used the model anyway. The node pause times varied between 0 s (high mobility) and 600 s (low mobility). For our simulations we used two scenario sizes. The small scenario had a size of 900 × 200 m and simulated 20 nodes. The larger scenario had a size of 1500 × 300 m and simulated 50 nodes. 4) Traffic Generation: Constant bit rate (CBR) sources have been used to model data traffic. The data packets had a size of 512 Byte. The simulation scenarios contained different numbers of data sources which were distributed randomly. In the small scenario either 4 or 16 sources have been used. In the large scenario either 10 or 20 sources were used. B. Selected Simulation Results Due to space limitations only a small selection of results will be presented. The end-to-end delay comparison of the protocols already gives a good impression.

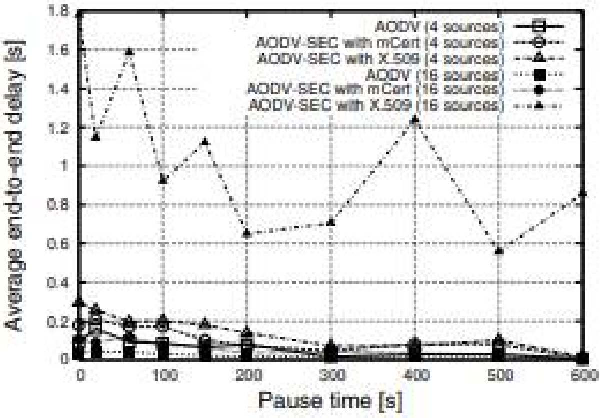

Fig. 3.1. Comparison of average end-to-end delay for data packets

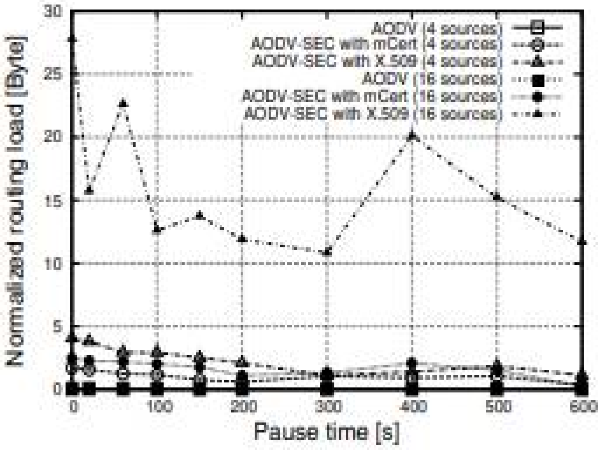

Fig. 3.2. Comparison of normalized routing load

On the capabilities and the drawbacks of the secure routing protocol. Especially in the small scenario with few source nodes the AODV-SEC performs well, almost as good as the regular AODV. Increasing the number of sources leads to a rather large increase of the end-to-end delay. Analyzing the effect of mobility shows that the end-to-end delay increases slightly with increasing mobility (refer to Fig. 1). Almost all of the three protocols perform very similarly and achieve an end-to-end delay for data packets between 0 s and 0.3 s. Only the AODVSEC protocol using X.509 certificates cannot achieve such short delays if the number of sources is large. The normalized routing load (NRL) results plotted in Fig. 2 also reflect the scalability issue of the X.509- version of the AODV-SEC protocol. In scenarios with few sources or the different AODV-SEC protocol implementation the NRL is much closer to the results of the insecure version of AODV.

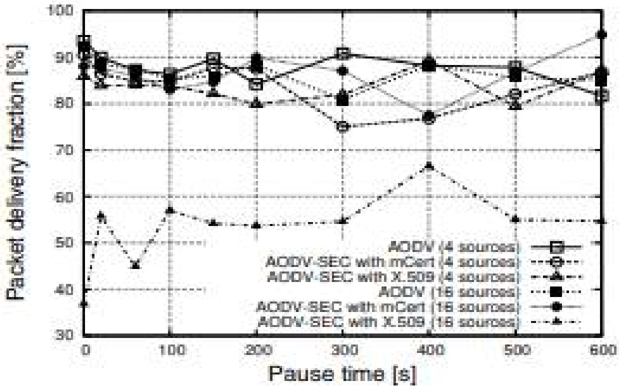

Fig. 3.3. Comparison of the packet delivery fraction

However, the NRL of almost 0 Byte can only be achieved by the insecure version of the protocol. The protocols using security show a rather significant routing overhead. A very significant parameter for the evaluation of a routing protocol is the packet delivery fraction (PDF). The PDF shows how successful a protocol performs delivering packets from source to destination. The higher the value the better. In Fig. 3 the results of the PDF for the three protocol implementations can be seen. The previous result's characteristics can also be recognized in this figure. The X.509-version of AODV-SEC doesn't scale well if the traffic load increases. All other protocol versions have a PDF between 80 % and 90 % or even better. This result demonstrates that a carefully designed secure version of AODV is indeed feasible. In Fig. 4 the simulation results for the end-to-end delay in the large simulation scenario can be seen. The regular AODV protocol scales well and has an acceptable delay between 0 s and 0.2 s for both load scenarios. This delay increases noticeably using the security extension. The AODV-SEC protocol achieves relatively long delays of up to 1.6 s for highly mobile scenarios (pause time 0 s). The delay decreases nearly exponentially for increasing pause times. Hence, the current implementation of AODV-SEC shows weaknesses in highly mobile scenarios with a high traffic load. Presumably this is caused by the larger packets and the delays due to the cryptographic mechanisms.

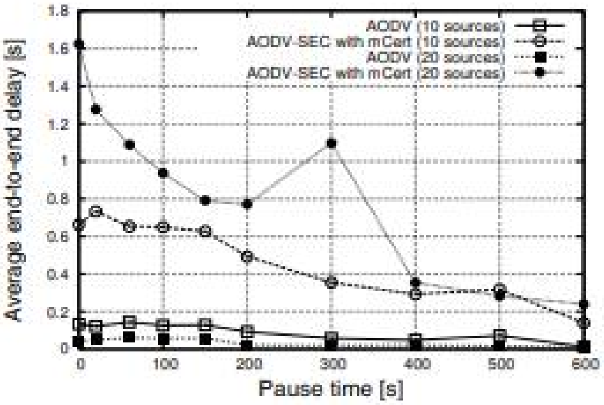

Fig. 3.4. Comparison of the end-to-end delay

CONCLUSION

MANET is a network which employing wireless sensor network technology. The performance is evaluated in terms of the end-to-end delay, Packet delivery ratio, residual energy and throughput. The AODV and MAOMDV routing protocols are implemented for both the standards. It is concluded that the MAOMDV is best suited for designing a enhanced quality oriented protocol for better throughput, Packet delivery ratio, Residual energy and larger coverage area with lower delay in multihop. The communication range of proposed network is according to WLAN standard i.e. 100m. It causes the performance degradation after this range. Thus, the work has to be extend further, in order to increase the coverage area. Every single routing protocol has its own advantages and disadvantages. No routing protocol can perform best in every type of network and scenario. So there is a need to develop new routing protocol, it could give higher performance with respect to quality of services in adhoc network it can also consider some other network parameters also those parameters are Packet Delivery Ratio and Residual Energy. The paper presents a selection of analysis results for the secure routing protocol AODV-SEC. The implementation of the protocol has been done using real cryptographic functions to be able to estimate the real performance using the simulator NS-2. The simulation results prove the feasibility of secure routing protocols, however, they point out that packet size and therefore the selection of cryptographic mechanisms and the certificate type is crucial for the performance of the protocol. The proposed work will be simulated in ns2. In future, it can be implemented in real time applications.

REFERENCES

1. 2016 Symposium on Colossal Data Analysis and Networking (CDAN) Multipath Routing Protocol for Mobile Adhoc Networks.
2. Challenges of Secure Routing in MANETs: A Simulative Approach using AODV-SEC Stephan Eichler and Christian Roman Institute of Communication Networks
3. Anonymity based Secure Cross layer Routing Protocol for Mobile Adhoc Networks.
4. 2012 International Conference on Computer Communication and Informatics (ICCCI -2012)
5. Secure Zone Based Routing Protocol for mobile Adhoc Networks.
6. 2010 Second International conference on Computing, Communication and Networking TechnologiesSecurity aware Minimized Dominating Set basedRouting in MANET.