MANET : SAODV v/s TAODV

Mr. Noman Rayeen[1], Prof. Chetana Khetmal[2]
K.C. College of Engineering & Management Studies & Research, Thane.
[1]synapselinked@gmail.com,[2]khetmalchetana@gmail.com

Abstract - The trade-off between strong cryptographic security and DoS has become increasingly important as MANET applications are developed which require a protocol with reasonable security and reasonable resistance to DoS, a kind of middle-ground. It has been suggested that various trust mechanisms could be used to develop new protocols with unique security assurances at different levels in this trade-off. However, the arguments for this have been purely theoretical or simulation-based. Determining the actual span of this trade-off in real world implementations is of utmost importance in directing future research and protocol design.

Keywords
MANET,SAODV, TAODV, Sender, Receiver,Intermediate Node etc.

I. INTRODUCTION

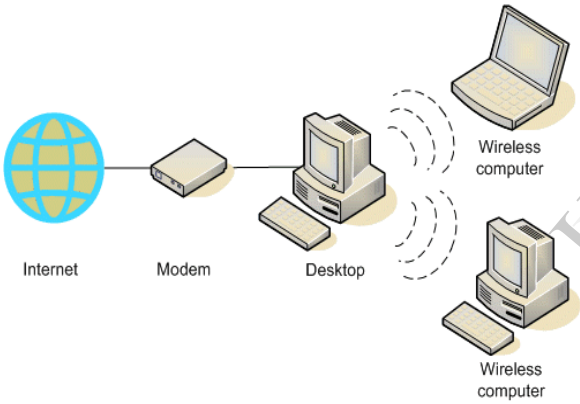

Figure 1 : MANET (Mobile Ad-hoc NETwork)

"A **mobile ad hoc network** (**MANET**), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links."[1]

Initial MANET routing protocols, such as AODV were not designed to withstand malicious nodes within the network or outside attackers nearby with malicious intent. Subsequent protocols and protocol extensions have been proposed to address the issue of security. Many of these protocols seek to apply cryptographic methods to the existing protocols in order to secure the information in the routing packets. It was quickly discovered, however, that whilesuch an approach does indeed prevent tampering with the routing information, it also makes for a very simple denial of service (DoS) attack . This attack is very effective in MANETs as the devices often have limited battery power in addition to the limited computational power. Consequently, this type of DoS attack allows for an attacker to effectively shutdown nodes or otherwise disrupt the network.

It is in this context that this paper considers two proposed protocol extensions to secure MANET routing. "The first, SAODV, uses cryptographic methods to secure the routing information in the AODV protocol. The second, TAODV, uses trust metrics to allow for better routing decisions and penalize uncooperative nodes."[2]. While some applications may be able to accept SAODV's vulnerability to DoS or TAODV's weak preventative security, most will require an intermediate protocol tailored to the specific point on the DoS/security trade-off that fits the application. The tailored protocols for these applications will also require performance that falls between that of SAODV and TAODV. Understanding how the SAODV and TAODV protocols (which are on the boundaries of the DoS/security trade-off) perform on real hardware, and to what extent there exists a performance gap is a prerequisite for being able to develop the intermediate protocols. Such evaluation is not only required for developing intermediate protocols, but also for determining the direction for development of new trust metrics for ad-hoc networks. In this paper we provide the first performance evaluations for these protocols on real world hardware.

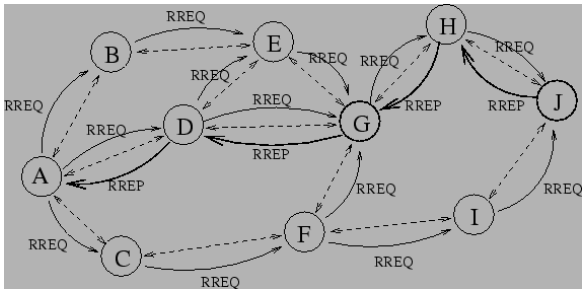

Figure 2: A possible path for a route reply if A wishes to find a route to J**.**

II. MANET ROUTING PROTOCOLS

Reactive protocols – AODV

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.

"The ***Ad-Hoc On-Demand Distance Vector*** **routing protocol** is described in RFC 3561. The philosophy in AODV, like all reactive protocols, is that topology information is only transmitted by nodes on-demand"

[3].When a node wishes to transmit traffic to a host to which it has no route, it will generate a *route request*(RREQ) message that will be flooded in a limited way to other nodes. A route is considered found when the RREQ message reaches either the destination itself, or an intermediate node with a valid route entry for the destination. For as long as a route exists between two endpoints, AODV remains passive. When the route becomes invalid or lost, AODV will again issue a request.

AODV defines three types of control messages for route maintenance:

RREQ - A *route request* message is transmitted by a node requiring a route to a node. Every RREQ carries a *time to live* (TTL) value that states for how many hops this message should be forwarded. This value is set to a predefined value at the first transmission and increased at retransmissions. Retransmissions occur if no replies are received.

RREP - A *route reply* message is unicasted back to the originator of a RREQ if the receiver is either the node using the requested address, or it has a valid route to the requested address. The reason one can unicast the message back, is that every route forwarding a RREQ caches a route back to the originator.

RERR - Nodes monitor the link status of next hops in active routes. When a link breakage in an active route is detected, a RERR message is used to notify other nodes of the loss of the link. In order to enable this reporting mechanism, each node keeps a ``precursor list'', containing the IP address for each its neighbors that are likely to use it as a next hop towards each destination.

III. SAODV

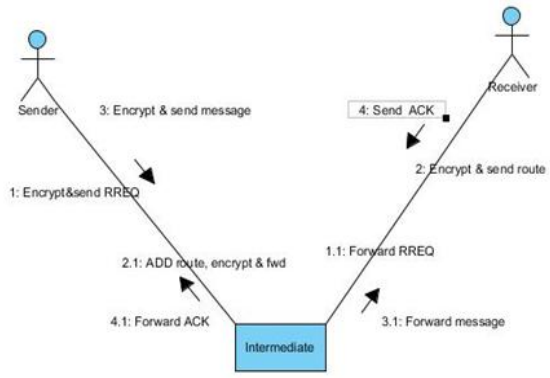

Figure 3 : SAODV (Secure Ad-hoc On-demand Distance Vector)

SAODV has three modules.

- Sender
- Intermediate node
- Receiver

Sender

Sender node is one which wants to send message to some other node. In SAODV whenever a sender want to send a message to some node, first it sends a route request to its neighbours and waits for reply. This route request is encrypted before being sent to neighbours. Once a neighbor sends the route reply, the sender has to decrypt the message given by neighbor using neighbour's key to view the route. After getting the route, the sender encrypts the message along with route and forwards to receiver and waits for acknowledgement. Once the acknowledgement is received by neighbor, it confirms that the message is delivered successfully to neighbor.

Intermediate node

The role of intermediate node is to exchange the route requests and message between the sender and receiver. When the intermediate node gets the route request from sender, it is encrypted. Intermediate node has to decrypt to route request using sender's key to know the destination's name. then it forwards the request to destination. Again it gets the reply for route from destination which is encrypted by destination node. The intermediate node decrypts the route reply and appends its address to it and again encrypts using its own key and forwards to the sender. When sender sends the message to intermediate node, the route will be in encrypted form. The intermediate node decrypts the route and checks the next node to which it has to forward the message and forwards it.

Receiver

The receiver node is one which receives the message from sender. When receiver gets the route request, it is encrypted by sender. The receiver decrypts the route request and views it, then it encrypts the route reply and forwards to sender. Again when sender sends message, it will be in encrypted form. The receiver decrypts the message and views it, then it sends an acknowledgement to sender.

IV. TAODV

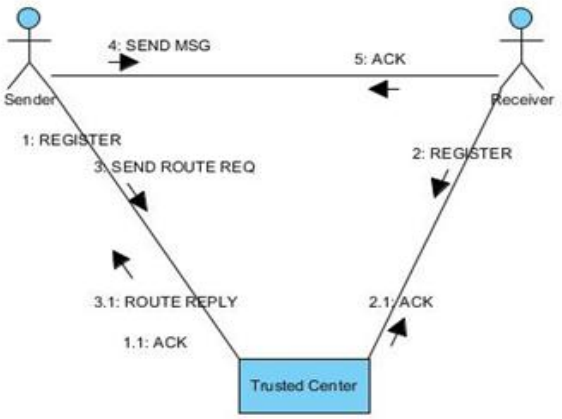

Figure 4 : TAODV (Trusted Ad-hoc On-demand Distance Vector)

TAODV contains four modules.

- Trusted Center
- Sender
- Intermediate node
- Receiver

Trusted Center

Trusted Center(TC) is a trusted node or router. "The role of TC is to store the routes available for all the registered nodes and send the route to a node whenever it requests for it. If a node gets registered with TC, it finds all the possible routes from the registered node to other nodes and

viceversa. If a node gets unregistered, TC removes the routes which contain unregister nodes address."[4].

Sender

In TAODV everything happens on basis of trust. Whenever a sender has to send message to receiver, first it has to get registered with TC. When sender wants to send message to receiver, it sends a route request to TC and TC sends the route reply. Then the sender sends the message to receiver using that route and waits for acknowledgement. Once it gets acknowledgement for message.

Intermediate node

This node gets the message from sender and forwards to receiver. Again it gets acknowledgement from receiver for sent message and forwards it to sender. This node also to be registered in TC.

Receiver

The receiver is one who gets the message from sender. Once it gets the message from some sender, it sends acknowledgement for it. The receiver should also be registered with TC to receive message from sender.

V. IMPLEMENTATION SCENARIO

In this implementation we have considered 4 static nodes. Each node can act as a sender, receiver or intermediary node. A separate node has been implemented to act as the Trusted Center in case of TAODV mode.

The nodes are implemented using socket programming in Java and Swings architecture.

TCP traffic will be used to send the packets.

VI. ANALYSIS ON TIME TAKEN TO SEND MESSAGE

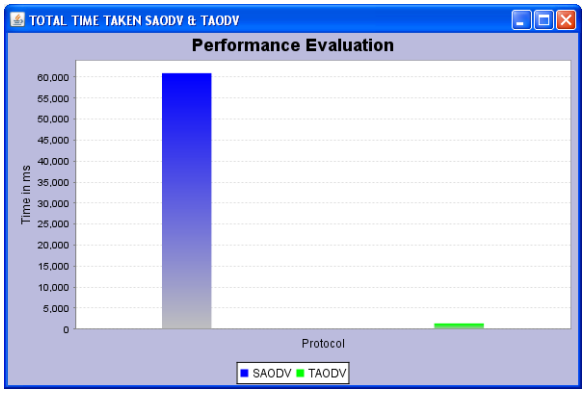

Figure 5 : Graph of Time Take to Send Message SAODV v/s TAODV

The above graph shows that the time taken to send a message using SAODV protocol is significantly larger than using TAODV protocol. This is because in SAODV mode, the message is encrypted by the sender node before sending and is decrypted by the receiver node. In TAODV mode there is no need to encrypt the message as it is assumed that since a node is registered in the trusted center it cannot be malicious.

VII. CONCLUSION

In this paper, we have compared the SAODV and TAODV protocols for securing adhoc network routing. We try to present the results of implementation and evaluation of both protocols on real resource-limited hardware. The aim of this simulation is to show that there is significant room between the two protocols for a secure hybrid protocol to be developed which takes advantage of the strongest points of both.

VIII. FUTURE WORK

Future work needs to delve further into the extensive body of work on various trust metrics. In addition, it is necessary to test the quality of the routing decisions produced by all of these protocols in a malicious environment.

REFERENCES

[1] J. Lundberg. Routing security in ad hoc networks, 2000.
[2] L. Zhou and Z. J. Haas.Securing ad hoc networks. IEEE Network, 13(6):24–30, 1999.
[3] H. Deng. Routing security in wireless ad hoc networks, 2002.
[4] Ethereal - A Network Protocol Analyzer. http://www.ethereal.com/
[5] http://homepages.inf.ed.ac.uk
[6] http://googlesystem.blogspot.com
[7] http://www.tested.com
[8] OpenZaurus. http://www.openzaurus.org/
[9] OpenSSL. http://www.openssl.org/
[10] http://en.wikipedia.org