Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 2, February 2015, pg.225 – 229

SURVEY ARTICLE

Comparative Study of Secured Routing Protocols in Wireless Ad hoc Networks: A Survey

Jyoti Neeli[1], Dr. N K Cauvery[2]

[1]Department of ISE Global Academy of technology Bangalore, India

[2]Department of ISE, RV College of Engineering Bangalore, India

[1] jyo_neeli@yahoo.co.in; [2] cauverynk@rvce.edu.in

***Abstract:** Wireless ad hoc networks are a collection of wireless nodes that communicate with each other without using any fixed infrastructure. Each of the nodes in the network participates as a router for forwarding packets from one node to another. Routing protocols designed for varying infrastructure are capable of withstanding ad hoc nature such as mobility and less bandwidth. Early routing protocols for MANETs failed to take security issues into account. Subsequent proposals used strong cryptographic methods to secure the routing information [1]. Routing in wireless ad hoc networks involves: determining optimal routing paths and transferring the packets through an internetwork. This paper discusses about AODV and TAODV routing protocols.*

***Keywords**— AODV, SAODV, TAODV*

I. Introduction

In Ad Hoc networks nodes communicate with each other without the intervention of centralized access points or base stations, so each node acts as a router and host. MANETS are infrastructure less, instantaneous networks. Use of Multihops enhances the transmission range in wireless ad hoc networks. MANETS have the feature of transmitting all signals through bandwidth constrained wireless links, nodes travel independently and in any direction, decentralized decisions make nodes to participate and cooperate. Nodes rely on batteries or other exhaustive means for energy.

This paper is structured as follows; Section II discusses classification of routing protocols Section III discusses AODV and some of the earliest MANET routing protocols; Section IV the Conclusion.

When routing protocols are designed for ad hoc network, various characteristic needed to be considered such as mobility of nodes in a network. Nodes are free to move randomly in a network and speed of mobility is not predicted before. Other important feature that needs to be considered that wireless channel provides lower and more variable bandwidth than wired network. So routing protocols should be bandwidth efficient thus by maintaining a minimum overhead for comparing routes so that much of the remaining bandwidth is available for the data packets. Similarly as nodes are running on batteries, in order to stay and communicate for longer periods, it is desirable that a routing protocol be energy efficient as well [2].

II. Classification of Routing Protocols

Routing protocols in ad hoc environment can be classified as Proactive routing protocol and Reactive routing protocol. Proactive protocols maintain routing tables of known destination thereby reducing control traffic overhead and wastage of bandwidth. In reactive routing protocol, route is established only when a source node needs to send data packet. AODV protocol falls under this category, as ad hoc by nature keeps on changing the network topology, this protocol in unsuitable as it needs routing table updates and thus degrades network performance with increased message overheads.

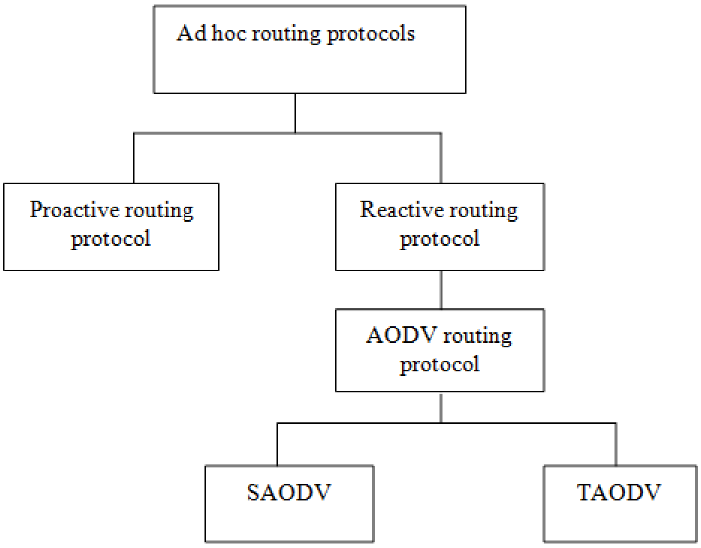

Fig 1: Classification of routing protocols

III. Routing Protocols based on AODV

AODV is a source initiated, reactive distance vector routing protocol, with nodes having same importance and functionality. Protocol makes use of Route request and Route reply messages to discover the routing path. An intermediate node that receives a RREQ replies to it using a route reply message only if it has a route to the destination whose corresponding destination sequence number is greater or equal to the one contained in the RREQ. This effectively means that an intermediate node replies to a RREQ only if it has a fresh enough route to the destination. Otherwise, an intermediate node broadcasts the RREQ packet to its neighbors until it reaches the destination. The destination unicasts a RREP back to the node that initiated the route discovery by transmitting it to the neighbor from which it received the RREQ [3]. Route maintenance process utilizes link-layer notifications, intercepted by neighboring nodes. Important feature of AODV is the maintenance of time-based states in each node: a routing entry not recently used is expired [4]. In case of a route is broken the neighbours can be notified. Disadvantage of this protocol is that intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries. Multiple Route Reply packets in response to a single RouteRequest packet can lead to heavy control overhead. Periodic beaconing leads to unnecessary bandwidth consumption, longer delay and greater packet loss when unsuccessful. Metrics used for calculating route between source and destination are based on freshness and length of the path i.e. the first received route is the shortest path .RREP contains sequence numbers implying freshness of the route.

Advantages of AODV

- As routes are created on demand basis , this minimizes number of broadcasts
- AODV does not put any additional overheads on data packets as it stores active path in intermediate nodes [5].
- Supports nodes in constant movement for both unicast and multicast packet transmissions, thereby responds very quickly to the topological changes that affects the active routes.

Limitations of AODV

- Approach uses shortest-path and static, i.e. the algorithms keep on using the same path, without considering its energy impact on the network, there by resulting in wastage of energy
- Path taken by the system imbalances the energy levels in the network and affect the connectivity of the network.
- Overhead involved is very high.

- Data packets delivered to too many nodes who do not need to receive them
- Potentially less reliable of data delivery
- Flooding uses broadcasting -- hard to implement reliable broadcast delivery without Significantly increasing overhead

A. Secure Ad-hoc on Demand Distance Vector Routing (SAODV)

SAODV is an extension to AODV, provides integrity, authentication and non repudiation of routing data. It uses asymmetric cryptography to secure AODV's routing messages. SAODV uses Digital Signatures to protect the non-mutable data in the RREQ and RREP messages. The four basic operations performed for the Route Establishment are: Route Discovery, Route Request,. Route Reply and .Route Maintenance. Before entering the network, each node obtains a public key certificate from a trusted certificate server. There are End-to-end authentication between source and destination and Hop-to-hop authentication between intermediate nodes. Hash chains are used in SAODV to authenticate the hop count of the AODV routing. Source broadcasts signed RDM (Route Discovery Message)[1] along with its own certificate. RDM contains the source IP address, along with a source-specific nonce (to detect duplicates).

First hop adds its own signature and certificate. Each hop verifies signature of previous hop and replaces it with its own signature also adds a reverse route to source. Destination also verifies the source signature [6]. In Route Reply the destination sends back a signed reply (RRM) to the first RDM. The discovered Route may not be the shortest, but is the "quickest". Route Maintenance Nodes send signed error messages (RERR) to indicate link breaks, and packets arriving on deactivated paths.

Hop count authentication by using hash chains is not perfect since a malign node might forward a message without increasing the hop count. Tunneling attacks are not solved by SAODV. The processing power requirements of SAODV should be reduced due to the use of asymmetric cryptography.

B. Trusted Ad-hoc on Demand Distance Vector Routing (TAODV)

TAODV uses trust metrics to allow for better routing decisions and penalize uncooperative nodes [7]. While some applications may be able to accept SAODV.s vulnerability to DoS or TAODV preventative security, most will require an intermediate protocol tailored to the specific point on the DoS security trade-off that fits the application [7]. The tailored protocols for these applications will also require performance that falls between that of SAODV and TAODV[1].TAODV uses trust relationship among nodes for routing, employ a trust model derived from subjective logic. Trust calculation is not time consuming and needs no digital signing for each routing messages.

C. Comparison of SAODV and TAODV

Simulation experiment carried out [8] shows that per packet overhead time for TAODV is very less compared to SAODV. Real world performance was measured by implementing on a real hardware. SAODV test requires generation and validation of SSE based on hash computation and digital signature/verification.

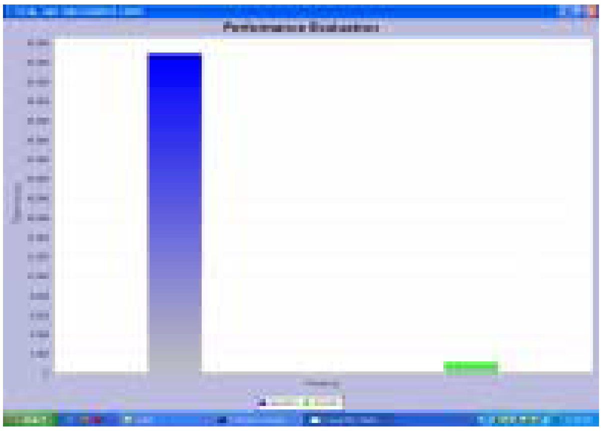

Fig 2: Comparison of SAODV and TAODV

Results also show that SAODV is significantly more expensive protocol. It takes 2.35 times as long as AODV to get RREP back to RREQ originator, because of added cryptography, increased message size and inability of intermediate nodes to respond to RREQs. On the other hand TAODV takes 1.11 times as long as AODV. Trust based calculations and additional information exchange can be used without incurring the overhead of SAODV. Results show that TAODV is indeed at the opposite end of the trade-off from SAODV. This is due to the fact that the TAODV information itself in each packet is not secured.

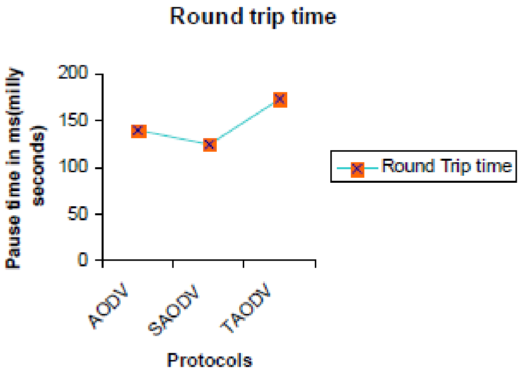

Fig 3:Round trip time

IV. Conclusion

Secured routing is one of the major tasks in MANETS. This paper reviewed various secure routing protocols based on AODV and from the comparative studies it is quite clear that these protocols are vulnerable to various routing attacks [9].

The performance of Trusted Ad-hoc On Demand Vector (TAODV) protocols has been analyzed by including the source route accumulation feature. Since MANET's have low transmission power, the transfer of data packet from one node to other implied threats due to malicious nodes.

Overall, the results show that there is indeed a wide spectrum in the tradeoff between cryptographic security and DoS[9]. By adding an appropriate lightweight security mechanism to secure the trust information in the routing packets, a hybrid protocol can be created which is less expensive than SAODV and more secure than TAODV [10]. Future protocol designs should seek [10] to use various new combinations of smarter, trust-based metrics and lightweight security [9] mechanisms in order to develop hybrid protocols across this spectrum.

References

[1] Jared Cordasco, Susanne Wetzel, "Cryptographic Versus Trust-based Methods for MANET Routing Security", *Electronic Notes in Theoretical Computer Science* 197(2008) 131–140.

[2] Farquad, "Routing in Mobile ad hoc networks", All *about Education* Jan 14, 2010.

[3] Stamouli, I. Argyroudis, P.G. ,Tewari, H, "Real-time intrusion detection for ad hoc networks", *World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium* 13-16 June 2005 page 374 – 380.

[4] Georgy Sklyarenko, "AODV Routing protocol", *Seminar Technische Informatik*.

[5] Mitul patel, Vasundhara V Uchhula , Bannishikha Banerjee "Comparative Evaluation of AODV, DSDV and AOMDV based on end-to-end delay and routing overhead using Network Simulator", (*IJCSIT) International Journal of Computer Science and Information Technologies* Vol.5 (2) ,2014 1638-1641.

[6] Rojith Thomas , Sreeja J. Kumar , Abhiram S , Aneesya C, "Modified trusted on demand routing protocol for secure spontaneous wireless ad-hoc network", *International Journal For Technological Research In Engineering* Volume 1, Issue 8, April-2014.

[7] Neetesh Saxena, Narendra S. Chaudhari, "Message Security in Wireless Networks: Infrastructure based vs. Infrastructure less Networks", 2012 IEEE.

[8] R.Balakrishna, U.Rajeswar Rao, M.S.Bhagyashekar, “Comparisons of SAODV and TAODV, DSR Mobile ad hoc network Routing Protocols”, *Int. J. Advanced Networking and Applications* Volume: 02 Issue: 01 Pages: 445-451 (2010).

[9] Dalip Kamboj, Pankaj Kumar Sehgal, “A Comparative Study of various Secure Routing Protocols based on AODV”, *(IJACSA) International Journal of Advanced Computer Science and Applications*, Vol. 2, No. 7, 2011.

[10] T Nagarjuna, C.C. Kalyan Srinivas, K R Arjun Reddy, “Implementation of SAODV and TAODVAdhoc Secure Routing Protocols”, *IJCSMC*, Vol. 2, Issue. 7, July 2013, pg.427 – 433.