International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Performance Evaluation of Secured Reactive Routing Protocols in MANETs

Shwetha T R [1], Arun Biradar[2]

[1, 2]Computer Science and Engineering Department, VTU Belgaum, EWIT, Bangalore, India

Abstract: ***A Mobile ad-hoc network (MANET) is mobile, multi-hop, infrastructure less wireless network which is capable of autonomous operation. Security is one of the biggest issue in MANETs as they are infrastructure-less and autonomous. Therefore, in MANET networks with security needs, there must be two considerations kept in mind: one to make the routing protocol secure and second one to protect the data transmission. Our endeavour in this paper would focus on achieving the routing and secure information exchange with the help of public key cryptography. This will facilitate the user nodes to perform routing, mutual authentications, generation and secure exchange of public and private keys. As a result of which ensuring confidentiality, integrity and authentication of data exchange in a more suitable and secured way.***

Keyword: Mobile ad-hoc network (MANET), On demand Distance Vector (AODV) Protocol, On demand Multipath Distance Vector (AOMDV), Routing, Security.

1. Introduction

An ad-hoc network is a collection of wireless mobile hosts forming a impermanent Network without the assistance of any stand-alone infrastructure or centralized administration. Mobile Ad-hoc networks are self-configuring and self-organizing multi hop wireless networks. Each node in mobile ad hoc networks is set up with a wireless transmitter and receiver, which permits it to communicate with other nodes in its communication range only. Nodes communicating usually share the similar physical media; they transmit and get signals at the same frequency band, and follow the same hopping sequence or spreading code. If the destination node is not inside the transmission range of the source node, the source node takes help of the intermediate nodes in order to communicate with the destination node by relaying the messages hop by hop.

Mobile wireless networks are generally open to various attacks, such as information and physical security attacks than fixed wired networks. Securing wireless ad hoc networks is particularly more difficult for many of the reasons such as: vulnerability of channels and nodes, absence of infrastructure, dynamically changing topology and etc. The wireless channel is accessible to both legitimate network users and malicious attackers. The abstract of centralized management makes the classical security solutions reliable on certification authorities and on-line servers not applicable. A malicious attacker can rapidly become a router and break network operations by deliberately not following the protocol specifications.

The nodes are free to move in any direction and organize themselves arbitrarily. They can join or leave the network at any time. Due to the frequently change in the network topology there is a significant change in the status of trust among different nodes which adds the complexity to routing among the various mobile nodes. The self-organization of nodes in ad hoc networks may tend to deny providing services for the advantage of other nodes in order to keep their own resources acquaint new security that are not addressed in the infrastructure-based networks.

2. Security Related Work

There have been many studies for security of routing in MANET. Hu et al. (2002b) proposed secure efficient ad hoc distance vector (SEAD) and used a protocol, which is based on the design of DSDV (Perkins & Bhagwat, 1994). SEAD is designed to prevent attacks such as DoS and resource consumption attacks. SEAD uses one way hash f unction for authenticating the updates, which are received from malicious nodes and non-malicious nodes and it can be used by any suitable authentication and key distribution scheme. However, finding such a scheme is not straightforward.

Ariadne (Hu et al., 2002a), by the same authors, is based on basic operation of DSR (Johnson & Maltz, 1996). Ariadne is a secure on-demand routing protocol and uses only high efficient symmetric cryptographic operations. Ariadne provides security against one compromised node and prevents many types of denial-of-service attacks. Ariadne uses message authentication code (MAC) and secret key shared between two parties to ensures point-to-point authentication of a routing message.

Security-aware routing (SAR) (Kravets et al., 2001) is an on demand routing protocol based on AODV (Perkins & Royer, 1999). SAR defines level of trust as a metric for routing. Nodes distribute key with those nodes having equal level of trust or higher level of trust. Thus an encrypted packet can be decrypted only by the nodes of the same or higher levels of trust. The main drawback of SAR is that during the path discovery process, encryption and decryption is done at each hop, which increases the power consumption. The protocol also requires different keys for various level of security, which leads to increase in number of keys required when the number of security levels used increases.

a) Exploring Ad Hoc On-Demand Distance Vector Routing (AODV):
AODV is an effective as well as a reactive routing protocol which has been designed for a MANET. AODV is a high-tech routing protocol that implements a purely reactive strategy. At the starting time of a communication session it

sets up a route on-demand, and uses it till it breaks, after that a new route setup is initiated. In AODV, when a source node S wants to send a packet to its destination node D and does not have a route to D, it begins its route discovery phase by broadcasting a route request message (RREQ) to its neighbor nodes. The route discovery phase of this protocol is shown in Figure.1.

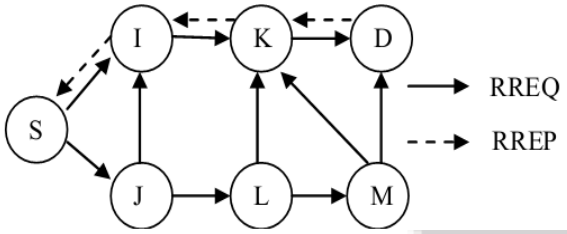


Figure 1: Route Discovery Process of AODV Routing Protocol

b)Exploring Ad Hoc-demand Multipath Distance Vector Routing (AOMDV):

on-demand multipath distance vector (AOMDV) is based on aprominent and well-studied on-demand single path protocol known as ad hoc on-demand distance vector AOMDV extends the AODV protocol to discover multiple paths between the source and the destination in every route discovery. Multiple paths so computed are guaranteed to be loop-free and disjoint. AOMDV has three novel aspects compared to other on-demand multipath protocols. First, it does not have high inter-nodal coordination overheads like some other protocols (e.g., TORA [3], ROAM [7]). Second, it ensures disjointness of alternate routes via distributed computation without the use of source routing. Finally, AOMDV computes alternate paths with minimal additional overhead over AODV; it does this by exploiting already available alternate path routing information as much as possible.

Loop Freedom:

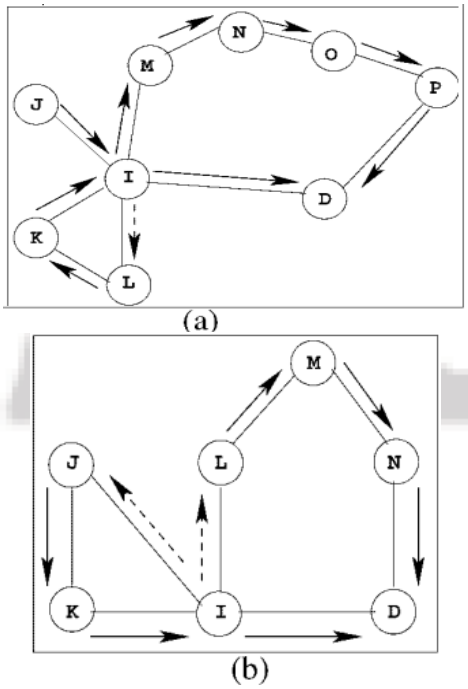


Figure 2: Examples of potential routing loop scenarios with multiple path computtin

Disjoint Paths

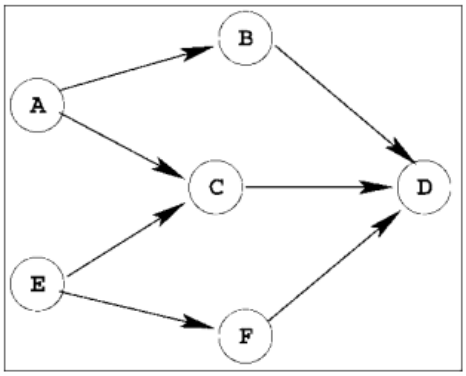


Figure 3: Paths maintained at different nodes to a destination may not be mutually disjoint. Here D is the destination. Node A has two disjoint paths to D: A – B – D and A – C – D .Similarly, node E has two disjoint paths to D : E – C – D and E – F – D . But the paths A – C – D and E – C – D are not disjoint; they share a common link C – D.

3. Proposed Work

The objective of proposed SAODV and AOMDV routing protocol is to secure routing packets of AODV and AOMDV protocol in MANET. The AODV and AOMDV protocol's routing have been improved to secure AODV and AOMDV. The proposed SAODV and AOMDV have three components. These are Hash Chain, Public Cryptography Algorithm (RSA), and Protocol Enforcement Mechanism.

1. Hash Chain used for securing the hop count
2. RSA for authentication
3. Protocol Enforcement Mechanism using the enforcement this protocol will address of any nodes,

Which packets have been changes?

The assumption of proposed SAODV routing protocol are:

1. The destination node can authenticate packets from the originator and each of receiving nodes can authenticate packets from the previous packets.
2. The hop count value is protecting using hash chain. It cannot be reduced by malicious node, but could be increased by one or retained unchanged.
3. Nodes in the network have capabilities for keys like private key, public key creation, signature generation and its verification.
4. Each node has one pair of keys (private key& public key). The RSA algorithm is well by the entire node in the network.

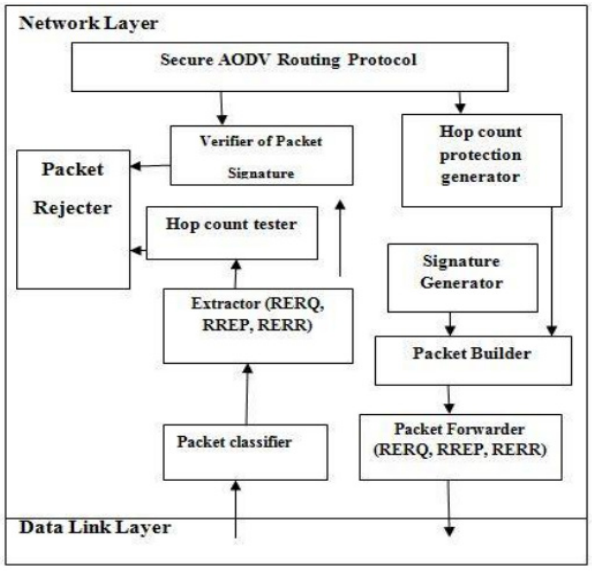


Figure 4: Architecture of Secure AODV and Secure AOMDV routing protocols

4. Simulation and Results

All simulation experiments are developed and simulated on an Intel(R) Core 2 Duo 1.83GHz machine using Ubuntu 12.4.0 with 2 GB RAM and the network simulator NS2 version NS allinone-2.35.

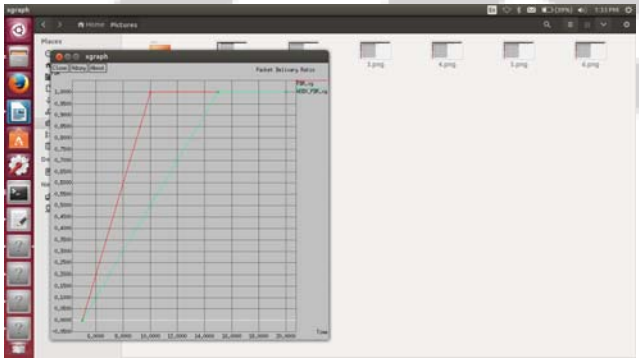
Table 1 summarizes the different configuration values that were used in all the performed simulations.

Table 1: General Simulation Parameters

Parameter	*Value*
Topology	1173*1000 m2
Number Of Nodes	27
Traffic type	CBR
Packet Size	256 bytes
Simulation	25 m/s
Node Speed	2.0 m/s
Transport Layer	UDP

Experiment 1: Packet Delivery Ratio

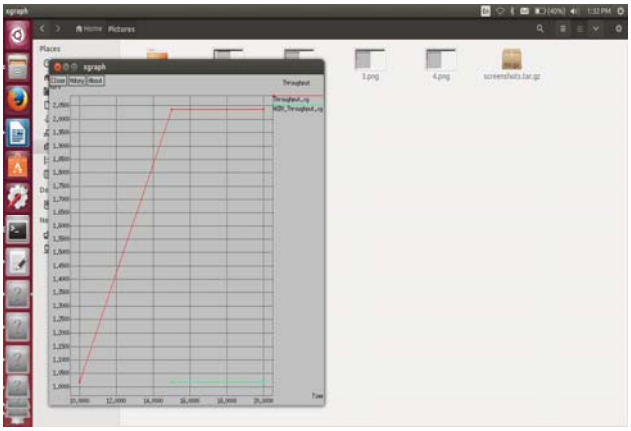
It is the ratio of packets delivered to that generated by the traffic generator. It is given by received packets/sent packets. The packet delivery ratio is directly influenced by packet loss, which may be caused by general network faults or uncooperative behaviour.



Packet Delivery Ratio Group for SAODV Vs SAOMDV

Experiment 2: Throughput

Throughput means packets received by intend receiver as per unit time denoted departure rate μ. Is measured bits/second



Throughput Group for SAODV Vs SAOMDV

5. Conclusion

In this paper the proposed approach uses improved of security mechanisms to introduce in the proposed techniques so that it satisfies the main security requirement and guarantees the discovery of a correct and secure route. The security mechanisms that the protocol uses are the hash chain, RSA Public Key Cryptography Algorithm and Protocol Enforcement Mechanism. The performance of these two protocols (SAODV and SAOMDV) was tested in simulation and their communication costs were measured using the NS-2 simulator, which was suitable for the present purpose. The evaluation metrics used in this study were Packet Delivery Ratio and end to Throughput, both the cases our protocol show better performance.

6. Acknowledgment

We express our heartfelt sincere gratitude to HOD of Computer Science and Engineering, East West Institute of Technology for his valuable suggestions and support. Special thanks to coordinator and guide for their valuable support and guidance.

References

[1] Abusalah, L., Khokhar, A., & Guizani, M. (2008). A Survey of Secure Mobile Ad Hoc Routing Protocols. IEEE Communications Surveys & Tutorial, 10 (4), 78-93
[2] Hu, Y. & Johnson, D.B. (2004). Securing Quality-of-Service Route Discovery in On-Demand Routing for Ad Hoc Networks. Proc. ACM SASN'04.
[3] Hu, Y.-C., Johnson, D.B. & Perrig, A. (2002a). Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks, Proceedings of Mobicom'02.
[4] Hu, Y., Perrig, A., & Johnson, D. (2002c). Packet Leashes: A Defense against Wormhole Attacks in Wire-less Networks. Proceedings of INFOCOM, IEEE
[5] Johnson, D., Hu, Y., & Malz, D. (2007). The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4. IETF, Request for Comments (RFC) 4728

[6] Sanzgiri, K., Dahill, B., Levine, B.N., Shields, C., & Belding-Royer, E. (2002). A secure routing protocol for ad hoc networks . Proceedings of the 10th International Conference on Network Protocols (ICNP'02)
[7] Singh, U. (2011). Secure Routing Protocol in Mobile Ad Hoc Networks – A Survey and Taxonomy. Inter-national Journal of Reviews in Computing, 7 (2), 9-17. Retrieved December 10, 2011 from http://www.ijric.org/volumes/Vol7/Vol7No2.pdf
[8] Yi, S, Naldurg, P., & Kravets, R. (2001). Security-Aware Ad hoc Routing for Wireless Networks. Second ACM Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc'01), 2001
[9] Zapata, M.G. & Asokan, N. (2002). Secure Ad ho c On-Demand Distance Vector (SAODV) Routing. ACM Mobile Computing and Communications Review, 3 (6), 106-107

Author Profile

Shwetha T.R, Completed B.E in Computer Science and Engineering at Nadgir institute of technology In Bangalore, Karnataka and currently pursuing the M.Tech degree in Computer Science and Engineering from East West institute of technology, Bangalore, Karnataka.

Prof Dr Arun Biradar, Currently working as HOD in computer science and engineering at East West institute of technology, Bangalore. He has more than 18 years of experience in teaching field. He is guiding M. Tech students in the area of Computer Networks, Wireless Networks. His professional activities are Chairman Indian Society for Technical Education (ISTE), Karnataka Section Board of Examiner (BOE) Member, VTU, Belgaum and Served as managing committee member ISTE Karnataka