Indian Journal of Science and Technology, *Vol 9(32), DOI: 10.17485/ijst/2016/v9i32/86261, August 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Performance Efficiency of SRP over AODV Enforcing Attacks

P. T. Kasthuri Bai* and M. Sundararajan

Bharathiar University, Coimbatore - 641046, Tamil Nadu, India; kasthuript@rediffmail.com, drmsrajan23@yahoo.com

Abstract

Objectives: Mobile ad hoc networks (MANETs) is a suitable environment for unknown or unspecified communications. It is an infra-structureless network. Standard protocols like AODV, OLSR and DSR are used in routing packets. In this paper, we compare AODV protocol with SRP protocol enforcing a Black hole, worm hole and Sybil attacks. Group signature is used to authenticate the route requests and to defend the potential active attacks without exposing the node identities. During the transmission, the intermediary nodes does not know the actual destination since onion routing concept along with route verification message is used. **Methods/Analysis:** Using NS2, first a sample of 50 nodes is generated and is made to move randomly. Dynamic clustering is done within the sample area of 500x500sq.m. Set up 50 nodes as sink nodes and attach a local agent and loss monitor for each node. Position these nodes in the sample area. The nodes 0,20,22,10 were set up as source and nodes 24,9,2,14 were set up as destinations respectively for transmission of packets. **Findings:** The four performance measures Energy spent, Packet Delivery ratio, delay and throughput or output with 6 attacker nodes (50,51,52,53,54,and 55)with different simulation time like 2,4,6,8,10s are taken for comparison. Transmission of packet is tested using AODV and the performance metrics are traced. Similarly the performance metrics are tested with SRP protocol. The values are tabulated and a graph is generated for each metric in Y-axis and time in X-axis. From the results obtained we can observe SRP outperforms AODV in all four parameters. **Novelty of the Study:** A VMware workstation is installed and tested in Unix environment using tool command language the modules are created in vi editor. They are executed using ns command. This paper compares the performance of SRP with AODV enforcing attacker nodes. **Conclusion:** During data transmission between nodes in MANETs the SRP protocol outperforms AODV. The result analysis below shows the four performance measures Energy spent, PDR, end-to-end delay and throughput.

Keywords: AODV (Adhoc Ondemand Distance Vector), Group Signature, SRP (Secured Routing Protocol), Unidentifiability, Unlinkability

1. Introduction

[1]Adhoc routing protocols have the properties like they operate in a Distributed manner, avoids packets spinning around in the network. They are proactive and it can adapt to traffic patterns on need basis and it also supports unidirectional link. There are some security issues in MANETs when they are used in military or battlefields due to its dynamic topology and open wireless medium. Even if the communications are encrypted, the attackers in the battlefield can infer the information about the intermediatary nodes or traffic flow. The trusted nodes can be captured by enemies and becomes malicious. Unknown communications can be described as a combination of unidentifiability and unlinkability. Unidentifiability means that the source and destination nodes cannot be identified by other nodes. Unlinking means that these nodes are no more or no less related from the attacker's view. To achieve these two properties a secured routing protocol is developed. That is SRP.

To implement an unknown communications appropriate secured routing protocols are used. In adversarial environment in MANET, topology-based on-demand routing protocols are used. To design an unknown protocol, a direct method is to make the node as unknown by using on-demand ad hoc routing protocols,

**Author for correspondence*

such as AODV[2] and DSR. To achieve this, the unknown security associations have to be established among the source, destination, and every intermediate node along a route. The resulting protocols include SDAR[3], AnonDSR[4], MASK[5,6], and Discount-ANODR[7]. In all the above these protocols, we find that the concept of unidentifiability and unlinkability are not fully satisfied. ANODR focuses on Route REQuest and Route REPly which protects the node or route identities during a route discovery process. This paper provides combination of unidentifiability and unlinkability by using SRP.

In the paper titled Progressive Routing Protocol using Hybrid Analysis for MANETs two routing protocols (AODV and OLSR) are considered for their routing messages towards their destinations and have combined these most popular properties to formulate a Hybrid MANET routing protocol using the tool Exata Cyber 1.1 Emulator. In the paper[8] analyses QoS of MANET's cryptographic mechanisms between Symmetric, Asymmetric and Threshold Cryptography. Trapdoor is one common mechanism that is widely used in anonymous secure routing. In cryptographic functions, a trapdoor is a common concept that defines a one-way function between two sets[9]. This paper[10] deals with ant based routing optimization in MANETs. In the paper[11], it has been observed that route after link breakage is found to be best with AODV nth BR protocol. In paper[12] the Perfect Evidence (PE) model uses reputation value to obtain the possibility and necessity measures and isolate a node having perfect evidence in MANETs.

2. Proposed System

Adhoc On Demand Distance Vector is a reactive routing protocol and it is a standard protocol. As and when required the routes are created so as to minimize the number of broadcasts. Each mobile host acts as a specialized router, and routes are obtained on demand as and when required. The AODV routing algorithm is quite suitable for a dynamic self-starting network. Loop-free routes are provided by AODV even while repairing broken links. AODV uses symmetric links between neighboring nodes. Whereas the Secured Routing (SRP) protocol is an authenticated user defined protocol in which the intermediatary nodes are unidentifiable. While discovering the route, the source node broadcasts an RREQ packet to every node in the network. The destination node replies with an RREP packet back along the incoming path of the RREQ, on receiving RREQ from the sender.

2.1 Unknown Route Request

1) Source Node: The source node S will generate a new session key for the association between S and D. The route request is sent along with the group signature and onion of S which is a key encrypted onion created by S.
2) Intermediate node: The RREQ packet is flooded to all intermediate nodes. The intermediate node confirms the packet by its group public key. The intermediate node examines the timestamp to determine whether the packet has been already processed or not.
3) Destination node: When RREQ packet reaches destination D, D validates it similar to the intermediate node. D decrypts the session key. It comes to know that it is the destination of RREQ. The destination can obtain the session key. D gathers an RREP to reply the source node's RREQ packet.

2.2 Unknown Route Reply

1) Destination Node: When the destination receives the RREQ packet, D authenticates it similarly to the intermediate nodes. The destination sends RREP along with route secret key, onion(D) and a shared key.
2) Intermediate Node: Successful decryption makes the intermediate nodes to know RREP is valid and remains to decrypt the onion part. Route reply travels from the destination node and moves back to its previous node which is based on the layers in the onion routing.

The proposed system compares AODV with SRP. Out of the 56 nodes, two nodes are made as Black hole attacker nodes and other two nodes are set as Worm hole attacker nodes and the other two nodes are set as Sybil nodes. Now using the AODV the packet transmission is tested. Now the packet transmission using SRP with the same type of attacker nodes is tested.

3. Performance Parameter and Metrics

Using ns2 simulator, the two protocols are tested. To achieve the required Quality of Service various performance metrics are considered. The parameters considered and compared are throughput, PDR, energy spent, delay. Two nodes (50,51) are made as Black hole attacker nodes and other two nodes (52,53) are set as Worm hole attacker nodes and the other two nodes (54,55) are set as Sybil nodes.

4. Result Analysis

In this work the performance analysis is carried out in an adhoc network by varying simulation time and keeping network area and number of nodes as constant. Two protocols i.e. AODV and SRP with attacks are considered for the comparison.

A graph (Figure1) is plotted by taking time in x axis and PDR (packet delivery ratio) in y-axis. PDR = Number of packets received/ Number of packets sent.

The redline shows performance of AODV in which PDR degrades when the time increases. The Green line shows the performance of AODV with attacks. Initially the PDR increases and after some time due to the attacks the PDR drops down. The blue line shows SRP with attacks in which PDR remains the same even if the time factor increases.

The comparison on energy spent is shown in the graph (Figure2). The blue line shows the performance of SRP with attacks in which energy consumed increases slowly till 4s and after that it remains the same as the time increases and it is the minimum energy spent when compared to other two.

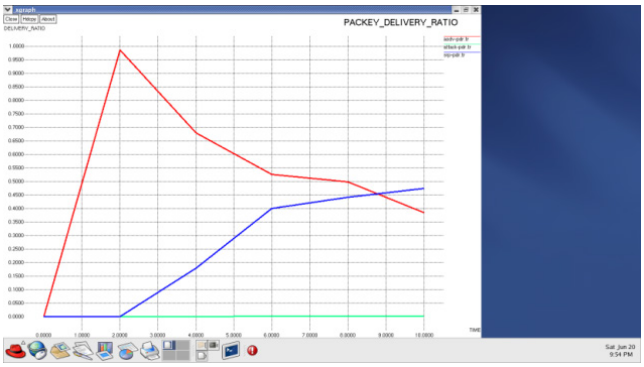

Figure 1. Packet Delivery Ratio.

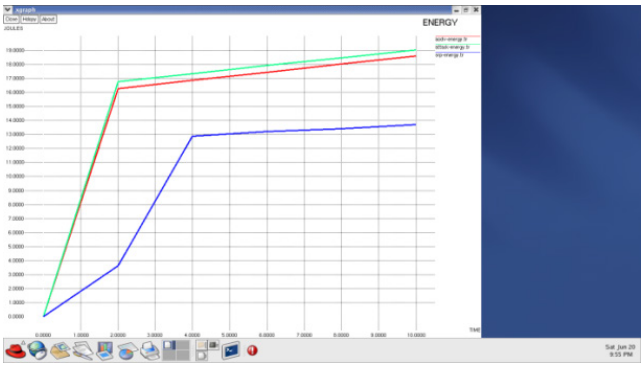

Figure 2. Energy Consumptions.

Throughput drops down slowly in case of AODV whereas the performance of SRP with attacks in which average packets received at the destination remains same after a period of time(Figure3).

In the Figure4, the redline shows performance of AODV in which delay increases gradually and remains the same afterwards. The delay is not uniform. The Greenline shows the performance of AODV with attacks in which

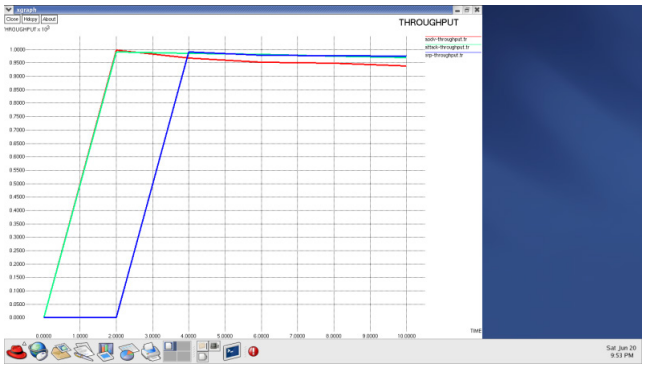

Figure 3. The average throughput rate.

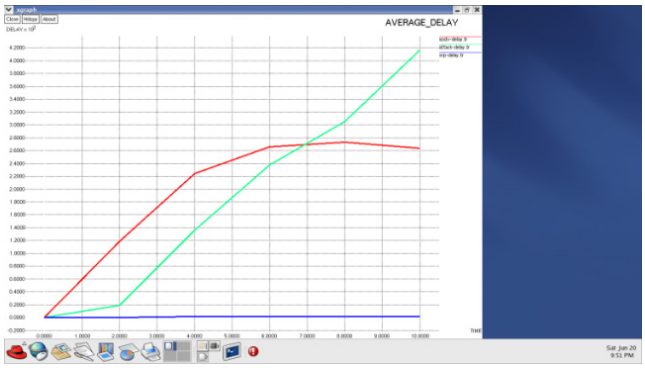

Figure 4. End-to-end delay.

Table 1. Parameters considered for the simulation in NS2

Parameters	Value
Type of network	Mobile Adhoc network
No. of nodes	56 nodes (6 attacker node)
Time Duration	0,2,4,6,8,10 s
MAC Protocol	MAC 802.11
Simulation area	500x500sq.m
Channel type	Wireless Channel
Antenna type	Omni Directional
Routing methods	AODV &SRP

delay gradually increases as the time increases also. The blue line shows the performance of SRP with attacks in which delay is negligible or there is no delay at all since the routing itself is authenticated and secured.

5. Conclusion

In this paper using NS2, the analysis of SRP and AODV protocol is done for the four parameters namely Energy spent, Packet delivery ratio, end-to-end delay and throughput. When malicious nodes attack the network, the performance of AODV protocol degrades. Whereas the performance of the network does not degrade while using SRP protocol. From the results obtained we can observe SRP outperforms AODV in all four parameters irrespective of simulation time. Further the wormhole, Sybil and black hole attacks do not degrade the performance of SRP protocols.

6. References

1. Sarkar S, Basavaraju TG, Puttamadappa C. Ad Hoc Mobile Wireless Networks: Principles, protocols and applications. Auerbach Publications, 2008.
2. Perkins, Belding-Royer E, Das S et al. RFC 3561 - Ad hoc On- Demand Distance Vector (AODV) Routing. Internet RFCs. 2003.
3. Boukerche A, El-Khatib K, Xu L, Korba L. SDAR: a Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad hoc Networks. Proceedings of IEEE Int'l Conf Local Computer Networks (LCN'04). 2004 Nov. p. 618–24.
4. Song R, Korba L, Yee G. AnonDSR: efficient anonymous dynamic source routing for mobile ad hoc networks. Proceedings ACM Workshop Security of Ad Hoc and Sensor Networks (SASN'05). 2005 Nov.
5. Zhang Y, Liu W, Lou W. Anonymous communications in mobile ad hoc networks. Proceedings IEEE INFOCOM. 2005 Mar; 3:1940–51.
6. Zhang Y, Liu W, Lou W, Fang YG. MASK: Anonymous On-Demand Routing in Mobile Ad hoc Networks. IEEE Trans on Wireless Comms. 2006 Sep; 5(9):2376–86.
7. Yang L, Jakobsson M, Wetzel S. Discount anonymous on demand routing for mobile ad hoc networks. Proceedings Int Conf on SECURECOMM'06. 2006 Aug.
8. Singh1 V, SaxenaA K. A Survey: QoS of MANET through cryptography and routing protocol enhancement. 2014 Feb; 3(2):225–31.
9. William S, Stallings W. Cryptography and Network Security, 4th Edition. Pearson Education India. 2006.
10. Persis DJ, Robert TP. Ant Based Multi-objective Routing Optimization in Mobile AD-HOC Network. Indian Journal of Science and Technology. 2015 May; 8(9):875–88.
11. Rao M, Singh N. Performance Evaluation of AODV nth BR Routing Protocol under Varying Node Density and Node Mobility for MANETs. Indian Journal of Science and Technology. 2015 Aug; 8(17):1–9. Doi:10.17485/indjst/2015/v8i17/70445.
12. Sahoo AJ, Akhtar AK. Possibility and Necessity Measures to Enhance Reliability and Cooperation in MANETS. Indian Journal of Science and Technology. 2014 Jan; 7(3):312–17. Doi:10.17485/indjst/2014/v7i3/47650.