Global Journal of Computer Science and Technology
Volume 12 Issue 5 Version 1.0 March 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

# Performance and Effectiveness of Secure Routing Protocols in Manet

By Er.Gurjeet Singh
*Desh Bhagat Institute of Engg & Management Moga*

*Abstract -* Mobile adhoc network (MANET) is a temporary network setup for a specific purpose without help of any preexisting infrastructure. The nodes in MANET are empowered to exchange packet using a radio channel. The nodes not in direct reach of each other uses their intermediate nodes to forward packets. (MANET) environment of MANET makes it vulnerable to various network attacks. A common type of attacks targets at the underlying routing protocols. Malicious nodes have opportunities to modify or discard routing information or advertise fake routes to attract user data to go through themselves. Some new routing protocols have been proposed to address the issue of securing routing information. However, a secure routing protocol cannot singlehandedly guarantee the secure operation of the network in every situation. The objectives of the paper is to study the performance and effectiveness of some secure routing protocols in these simulated malicious scenarios, including ARIADNE and the Secure Ad hoc On-demand Distance Vector routing protocol (SAODV).

*GJCST Classification: C.2.2*

# Performance and Effectiveness of Secure Routing Protocols in Manet

Er.Gurjeet Singh

*Abstract -* Mobile adhoc network (MANET) is a temporary network setup for a specific purpose without help of any pre-existing infrastructure. The nodes in MANET are empowered to exchange packet using a radio channel. The nodes not in direct reach of each other uses their intermediate nodes to forward packets. (MANET) environment of MANET makes it vulnerable to various network attacks. A common type of attacks targets at the underlying routing protocols. Malicious nodes have opportunities to modify or discard routing information or advertise fake routes to attract user data to go through themselves. Some new routing protocols have been proposed to address the issue of securing routing information. However, a secure routing protocol cannot single-handedly guarantee the secure operation of the network in every situation. The objectives of the paper is to study the performance and effectiveness of some secure routing protocols in these simulated malicious scenarios, including ARIADNE and the Secure Ad hoc On-demand Distance Vector routing protocol (SAODV).

## I. Introduction

Mobile Ad-hoc network is a set of wireless devices called wireless nodes, which dynamically connect and transfer information. Wireless nodes can be personal computers (desktops/laptops) with wireless LAN cards, Personal Digital Assistants (PDA), or other types of wireless or mobile communication devices. Figure 1 illustrates what MANET is. In general, a wireless node can be any computing equipment that employs the air as the transmission medium. As shown, the wireless node may be physically attached to a person, a vehicle, or an airplane, to enable wireless communication among them..

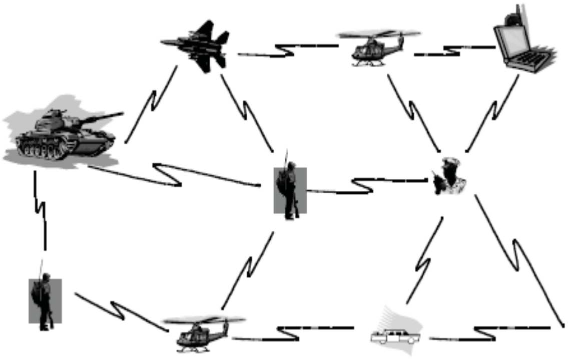
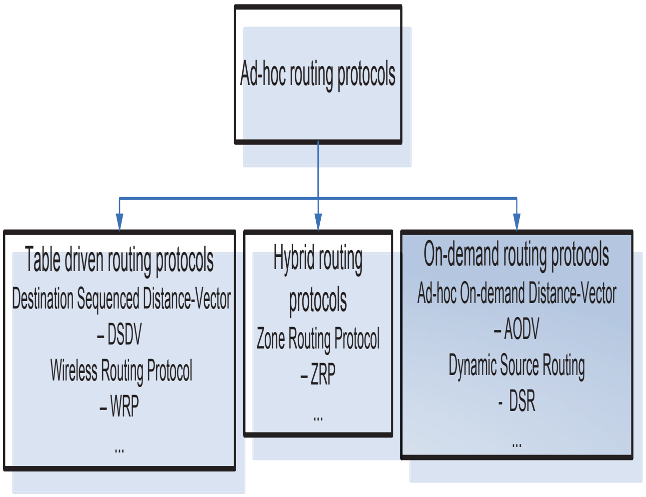


*Figure1:* Mobile Ad-hoc Network

*Author : AP, Deptt of CSE Desh Bhagat Institute of Engg & Management Moga*

## II. Adhoc Wireless Routing Protocols

Routing protocols in ad hoc mobile wireless network can generally be divided into three groups


Ad-hoc routing protocols
Table driven routing protocols
Destination Sequenced Distance-Vector
- DSDV
Wireless Routing Protocol
- WRP
...
Hybrid routing
protocols
Zone Routing Protocol
- ZRP
...
On-demand routing protocols
Ad-hoc On-demand Distance-Vector
- AODV
Dynamic Source Routing
- DSR
...

- **Table driven:** Every node in the network maintains complete routing information about the network by periodically updating the routing table. Thus, when a node needs to send data packets, there is no delay for discovering the route throughout the network. This kind of routing protocols roughly works the same way as that of routing protocols for wired networks.
- **Source initiated (or demand driven):** In this type of routing, a node simply maintains routes to active destination that it needs to send data. The routes to active destinations will expire after some time of inactivity, during which the network is not being used.
- **Hybrid:** This type of routing protocols combines features of the above two categories. Nodes belonging to a particular geographical region or within a certain distance from a concerned node are said to be in the routing zone and use table driven routing protocol. Communication between nodes in different zones will rely on the on-demand or source-initiated protocols.

## III. Dynamic Source Routing Protocol(DSR)

The Dynamic Source Routing Protocol is one of the on-demand routing protocols, and is based on the concept of *source routing*. In source routing, a sender node has in the packet header the complete list of the path that the packet must travel to the destination node. That is, every node in the path just forwards the packet to its next hop specified in the header without having to check its routing table as in table-driven routing protocols. Besides, the nodes don't have to periodically broadcast their routing tables to the neighboring nodes. This saves a lot of network bandwidth. The two phases of the DSR operation are described below:

- Route Discovery phase

In this phase, the source node searches a route by broadcasting route request (RREQ) packets to its neighbors. Each of the neighbor nodes that has received the RREQ broadcast then checks the packet to determine which of the following conditions apply: (a) Was this RREQ received before ? (b) Is the TTL (Time To Live) counter greater than zero? (c) Is it itself the destination of the RREQ? (d) Should it broadcast the RREQ to its neighbors? The *request ids* are used to determine if a particular route request has been previously received by the node. Each node maintains a table of RREQs recently received. Each entry in the table is a *<initiator, request id>* pair. If two RREQs with the same *<initiator, request id>* are received by a node, it broadcasts only the one received first and discards the other. This mechanism also prevents formation of routing loops within the network. When the RREQ packet reaches the destination node, the destination node sends a reply packet (RREP) on the reverse path back to the sender. This RREP contains the recorded route to that destination.

Figure 2 shows an example of the route discovery phase. When node A wants to communicate with node G, it initiates a route discovery mechanism and broadcasts a request packet (RREQ) to its neighboring nodes B, C and D as shown in the figure. However, node C also receives the same broadcast packets from nodes B and D. It then drops both of them and broadcasts the previously received RREQ packet to its neighbors. The other nodes follow the same procedure. When the packet reaches node G, it inserts its own address and reverses the route in the record and unicasts it back on the reversed path to the destination which is the originator of the RREQ.

The destination node unicasts the best route (the one received first) and caches the other routes for future use. A *route cache* is maintained at every node so that, whenever a node receives a route request and finds a route for the destination node in its own cache, it sends a RREP packet itself instead of broadcasting it further.

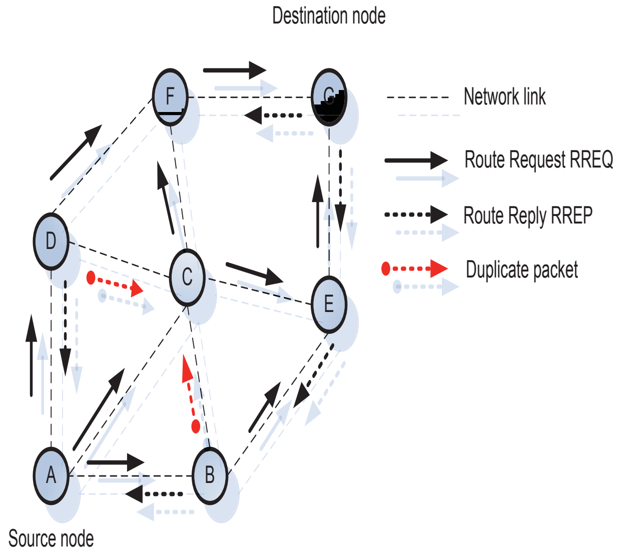


*Figure 2:* Route Discovery in DSR

- Route Maintenance

The route maintenance phase is carried out whenever there is a broken link between two nodes. A broken link can be detected by a node by either passively monitoring in promiscuous mode or actively monitoring the link. As shown in Figure 3, when a link break (F-G) happens, a route error packet (RERR) is sent by the intermediate node back to the originating node. The source node re-initiates the route discovery procedure to find a new route to the destination. It also removes any route entries it may have in its cache to that destination node.

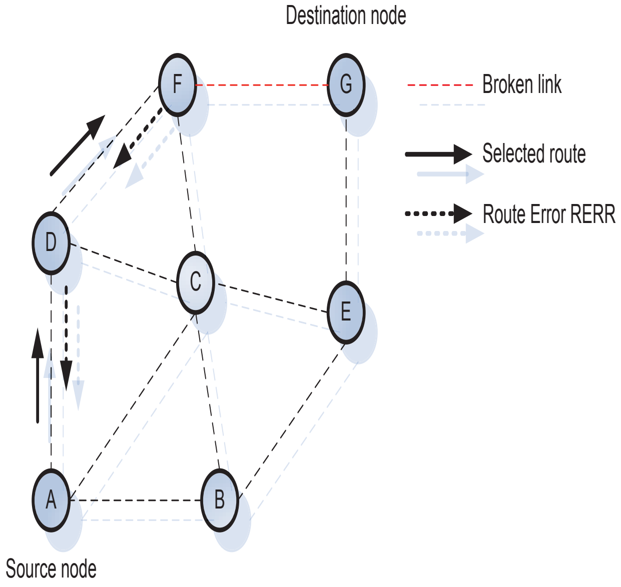


*Figure3:* Route Maintenance in DSR

DSR benefits from source routing since the intermediate nodes do not need to maintain up-to-date routing information in order to route the packets that they receive. There is also no need for any periodic routing advertisement messages. However, as size of the network increases, the routing overhead increases since each packet has to carry the entire route to the destination along with it. The use of route caches is a good mechanism to reduce the propagation delay but overuse of the cache may result in poor performance [7]. Another issue of DSR is that whenever there is a link break, the RERR packet propagates to the original source, which in turn initiates a new route discovery process. The link is not repaired locally. Several optimizations to DSR have been proposed, such as non- propagating route requests (when sending RREQ, nodes set the hop limit to one preventing them from re-broadcasting), gratuitous route replies (when a node overhears a packet with its own address listed in the header, it sends a RREP to the originating node bypassing the preceding hops), etc.

## IV. Adhoc On Demand Distance Vector (AODV) Routing Protocol

To find routes, the AODV routing protocol [9] uses a reactive approach and to identify the most recent path it uses a proactive approach. That is, it uses the route discovery process similar to DSR to find routes and to compute fresh routes it uses destination sequence numbers. The two phases of the AODV routing protocol are described below.

- Route Discovery

In this phase, RREQ packets are transmitted by the source node in a way similar to DSR. The components of the RREQ packet include fields such as the source identifier (SId), the destination identifier (DId), the source sequence number (SSeq), the destination sequence number (DSeq), the broadcast identifier (BId), and TTL. When a RREQ packet is received by an intermediate node, it could either forward the RREQ packet or prepare a Route Reply (RREP) packet if there is an available valid route to the destination in its cache. To verify if a particular RREQ has already been received to avoid duplicates, the (SId, BId) pair is used. While transmitting a RREQ packet, every intermediate node enters the previous node's address and its BId. A timer associated with every entry is also maintained by the node in an attempt to delete a RREQ packet in case the reply has not been received before it expires.

When a node receives a RREP packet, the information of the previous node is also stored in it in order to forward the packet to it as the next hop of the destination. This plays a role of a "forward pointer" to the destination node. By doing it, each node contains only the next hop information; whereas in the source routing, all the intermediate nodes on the route towards the destination are stored.

Figure 4 depicts an example of route discovery mechanism in AODV. Suppose that node A wishes to forward a data packet to node G but it has not an available route in its cache. It then initiates a route discovery process by broadcasting a RREQ packet to all its neighboring nodes (B, C and D).

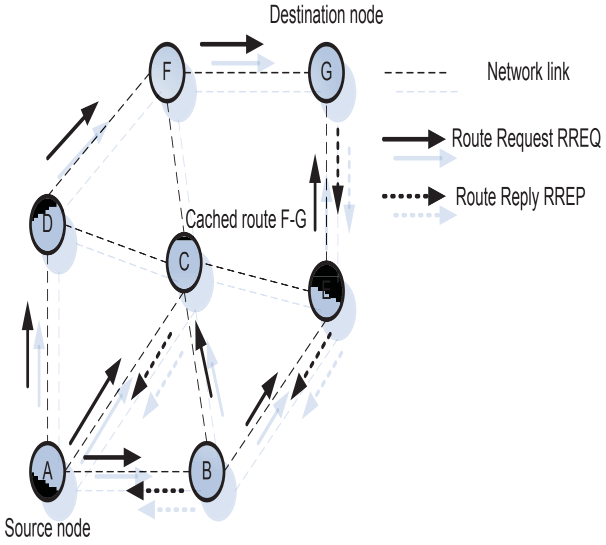


*Figure 4:* Route discovery in AODV

When RREQ packet reaches to nodes B, C and D, these nodes immediately search their respective route caches for an existing route. In the case where no route is available, they forward the RREQ to their neighbors; otherwise a comparison is made between the destination sequence number (DSeq) in the RREQ packet and the DSeq in its corresponding entry in the route cache. It replies to the source node with a RREP packet consisting of the route to the destination in the case the DSeq in the RREQ packet is greater.

- Route Maintenance

The way that the route maintenance mechanism works is described below. Whenever a node finds out a link break (via link layer acknowledgements or HELLO messages [9]), it broadcasts an RERR packet (in a way similar to DSR) to notify the source and the end nodes. This process is illustrated in Figure 5 If the link between nodes C and F breaks on the path A-C-F-G, RERR packets will be sent by both F and C to notify the source and the destination nodes.

The main advantage of AODV is the avoidance of source routing to reduce the routing overload in a large network. Another good feature of AODV is its application of expanding-ring-search to control the flood of RREQ packets and search for routes to unknown destinations [10]. In addition, it also supplies destination sequence numbers, allowing the nodes to have more up-to-date routes. However, some notes have to be taken into consideration when using AODV. Firstly, it requires bidirectional links and periodic link layer acknowledgements to detect broken links. Secondly, unlike DSR, it needs to maintain routing tables for route maintenance unlike DSR.

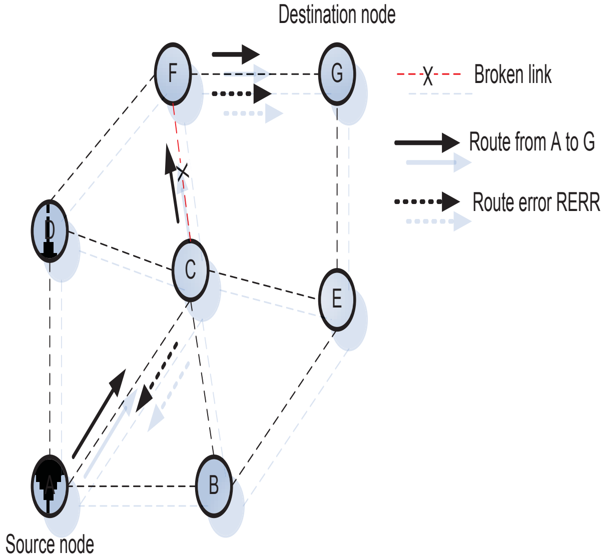


*Figure 5:* Route Maintenance in AODV

## V. Attacks On Existing Protocols

In general, the attacks on routing protocols can generally be classified as routing disruption attacks [14][15] and resource consumption attacks [14][15]. In routing disruption attacks, the attacker tries to disrupt the routing mechanism by routing packets in wrong paths; in resource consumption attacks, some non-cooperative or selfish nodes may try to inject false packets in order to consume network bandwidth. Both of these attacks are examples of Denial of Service (DoS) attacks. Figure 6 depicts a broader classification of the possible attacks in MANETs.

- Attacks using Modification

In this type of attacks, some of the protocol fields of the messages passed among the nodes are modified, thereby resulting in traffic subversion, redirection or Denial of Service (DoS) attacks. The following sections discuss some of these attacks.

○ *Modification of Route Sequence Numbers :* This attack is possible against the AODV protocol. The malicious node can change the sequence number in the route request packets or route reply packets in order to make the route fresh. In Figure 7, malicious node M receives a route request RREQ from node B that originates from node S and is destined for node X. M unicasts a RREP to B with a higher destination sequence number for X than the value last advertised by X. The node S accepts the RREP and then sends the data to X through M. When the legitimate RREP from X gets to S, if the destination number is less than the one advertised by M, then it will be discarded as a stale route. The situation will not be corrected until a valid RREP with higher sequence number than that of M gets to S.

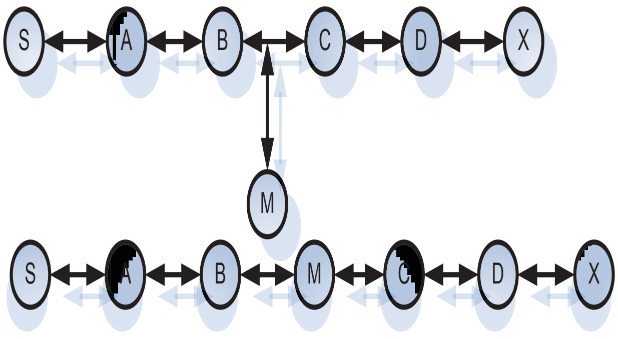


*Figure 7:* An example of route modification attack

○ *Modification of Hop Count :* This type of attacks is possible against the AODV protocol in which a malicious node can increase the chance that they are included in a newly created route by resetting the hop count field of a RREQ packet to a lower number or even zero. Similar to route modification attack with sequence number, the hop count field in the routing packets is modified to attract data traffic.

○ *Modification of Source Route :* This attack is possible against DSR which uses source routes and works as follows. In Figure 7, it is assumed that the shortest path exists from S to X. It is also assume that C and X cannot hear each other, that nodes B and C cannot hear each other, and that M is a malicious node attempting a denial-of-service attack. Suppose S sends a data packet to X with the source route S-A-B-C-D-X. If M intercepts this packet, it removes D from the list and forwards it to C. C will attempt to forward this packet to X which is not possible since C cannot hear X. Thus M has successfully launched a DoS attack on X.

- Attacks Using Impersonation

This type of attacks violates authenticity and confidentiality in a network. A malicious node can impersonate or spoof the address of another node in order to alter the vision of the network topology as perceived by another node. Such attacks can be described as follows in Figure 8

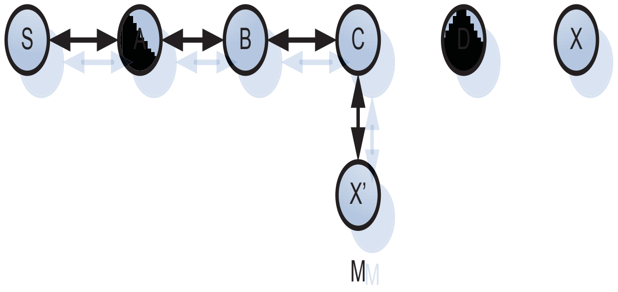


*Figure 8:* An example of impersonation attack

Node S wants to send data to node X and initiates a Route Discovery process. The malicious node M, closer to node S than node X, impersonates node X as X'. It sends a route reply (RREP) to node S. Without checking the authenticity of the RREP, node S accepts the route in the RREP and starts to send data to the malicious node. This type of attacks can cause a routing loop within the network.

- Special Attacks

In addition to the attacks described above, there are two other severe attacks which are possible against routing protocols such as AODV and DSR.

- ○ *Wormhole Attack* : The wormhole attack [11] is a severe type of attacks in which two malicious nodes can forward packets through a private "*tunnel*" in the network as shown in Figure 9.

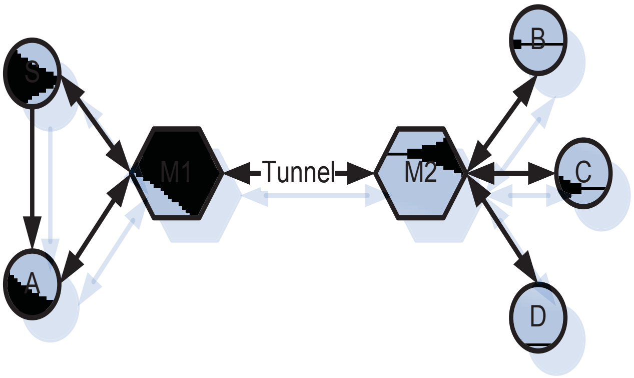


*Figure 9:*An example of wormhole attack

Here, $M_1$ and $M_2$ are two malicious nodes which link through a private connection. Every packet that $M_1$ receives from the network is forwarded through "wormhole" to node $M_2$, and vice versa. This attack disrupts routing protocols by short circuiting the normal flow of routing packets. Such a type of attack is difficult to detect in a network, and may severely damages the communication among the nodes. Such an attack can be prevented by using packet leashes [18], which authenticate the timing information in the packets to detect faked packets in the network.

- ○ *Black Hole Attack* : A node advertises a zero metric for all destinations causing all nodes around it to route data packets towards it. The AODV protocol is vulnerable to such an attack.

## VI. Experimental Results

The performance data of four routing protocols (DSR, ARIADNE, AODV and SAODV) are collected. A scenario is set up for data collection. This scenario is run 11 times with 11 different values of the mobility *pause time* ranging from 0 to 100 seconds. The data is collected according to two metrics

- Packet Delivery Fraction
- Normalized Routing Load

In general, the actual values of the performance metrics in a given scenario are affected by many factors, such as node speed, moving direction of the nodes, the destination of the traffic, data flow, congestion at a specific node, etc. It is therefore difficult to evaluate the performance of a protocol by directly comparing the acquired metrics from individual scenarios. In order to obtain representative values for the performance metrics, we decided to take the average values of multiple simulation runs. The average values of these 11 simulation runs are then calculated for the two metrics and used as a baseline to evaluate the performance of routing protocols in malicious environments.

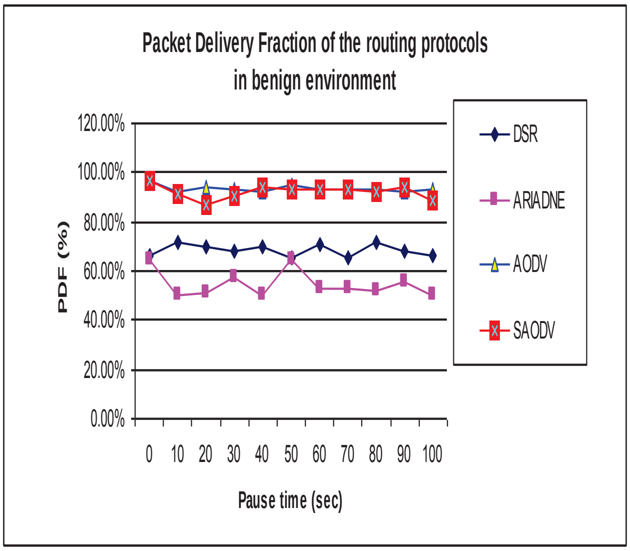


*Figure 10:*Packet Delivery Fraction vs. pause time values in benign environment

As shown in Figure 10 the percentage of packets delivered in AODV and SAODV is fairly close to each other, and both methods exhibit superior performance (~90% in general). The security features in SAODV lower the performance a little bit. Actually, the generation and verification of digital signatures depends on the power of the mobile nodes and causes a delay in routing packet processing. In the simulation environments, this delay depends on the simulation running machine and is not high enough to make the significant difference for the PDF metric. On the other hand, the packet delivery fraction in DSR and ARIADNE are 20-40% lower than that of AODV/SAODV across the board given different mobility pause times.

The major difference between AODV and DSR is caused by difference in their respective routing algorithms. It was reported by other researchers [5] [7] that, in high mobility and/or stressful data transmission scenarios, AODV outperforms DSR. The reason is that DSR heavily depends on the cached routes and lack any mechanism to expire stale routes. In the benign environment of our experiments, the default expiry timer of cached route for DSR and ARIADNE is 300 seconds, while this number is 3 seconds for AODV and SAODV. In respect to the protocol design, these values are kept unchanged through all the simulation scenarios. Furthermore, DSR and ARIADNE store the complete path to the destination. Hence, if any node moves out of the communication range, the whole route becomes invalid. In MANETs, the nodes are mobile, so route change frequently occurs. Without being aware of most recent route changes, DSR may continue to send data packets along stale routes, leading to the increasing number of data packets being dropped.

The situation is even worse for ARIADNE, mainly because ARIADNE relies on the delayed key disclosure mechanism of TESLA when authenticating packets, including the RERR packets. When an intermediate node in ARIADNE notices a broken link, it sends a RERR message to the source node of the data packet. The source node, however, simply saves the RERR message, because it has not yet received from the intermediate node the key needed to authenticate the route error. The source node keeps sending the data until the second route error is triggered, and another RERR is received. Only then would the previous route error be authenticated, and the broken link not be used any more. This explains the worse performance of ARIADNE in comparison with DSR and other protocols.

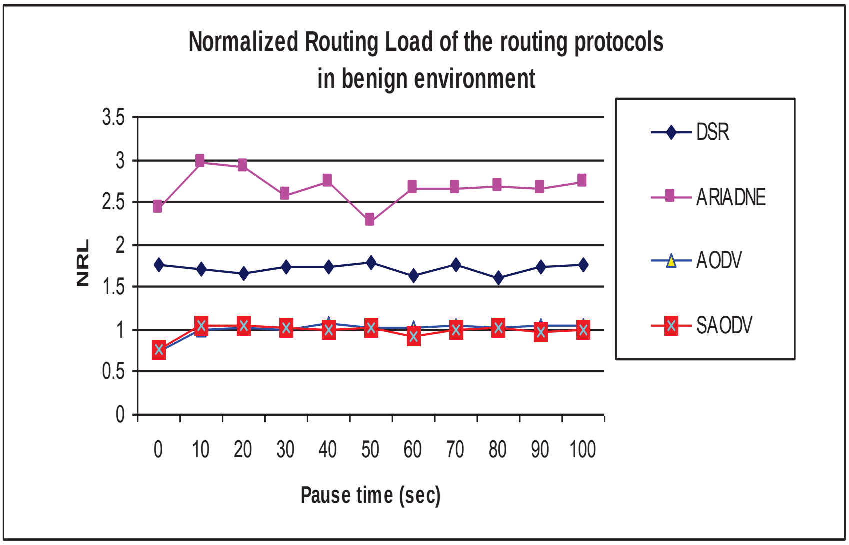


*Figure 11:* Normalized Routing Load vs. pause time values in benign environment

As shown in Figure 11, the NRL metric is, in general, inversely proportional to the PDF metric. A low PDF value corresponds to a high NRL value. This relationship between PDF and NRL is further illustrated in Table 1.1, which lists the average values of the two metrics over 11 simulation runs for each of the four protocols.

| Pause Time (seconds) | Packet Delivery Fraction (%) | Normalized Routing Load |
|---|---|---|
| DSR | 68.41% | 1.72 |
| ARIADNE | 54.70% | 2.58 |
| AODV | 93.45% | 1.01 |
| SAODV | 92.00% | 0.98 |

*Table 1.1* The “baseline” metrics of the four protocols

## VII. Conclusion

In this paper, I have implemented two secure routing protocols, ARIADNE and SAODV, based on their respective underlying protocols, DSR and AODV, in the OPNET simulation environment. I have also simulated four popular network attack models that exploit the weakness of the protocols. The attack models are used to make malicious wireless nodes and create various malicious environments, in which the performance of DSR, AODV, ARIADNE, and SAODV are evaluated. AODV and SAODV without pubic key verification are vulnerable to impersonation attacks. The impacts on the two protocols are similar. The more the number of malicious nodes in the network is, the fewer the number of received data packets is. As shown by the experiments, SAODV is secure against impersonation attack only when there is a way to verify the public key of the route reply originator. In other words, a key management center is really necessary to make SAODV secure against impersonation attacks. This is still an outstanding issue of SAODV. The ultimate goal of a routing protocol is to efficiently deliver the network data to the destinations; therefore, two metrics, Packet Delivery Fraction (PDF) used to evaluate the protocols.

## References Références Referencias

1. Yih-Chun Hu, Adrian Perrig, and David B. Johnson. "Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks". MobiCom 2002, September 23-28, 2002, Atlanta, Georgia, USA. http://www.ece.cmu.edu/~adrian/projects/secure routing/ariadne.pdf
2. Manel Guerrero Zapata. “Secure Ad hoc On-Demand Distance Vector Routing”. ACM Mobile Computing and Communications Review (MC2R), 6(3):106--107, July 2002. http://lambda.cs.yale.edu/ cs425/doc/zapata.pdf
3. Mishra Amitabh, Nadkarni Ketan M., and Ilyas Mohammad. “Chapter 30: Security in wireless ad-hoc networks, the handbook of Ad hoc wireless network”, CRC PRESS Publisher, 2003.
4. Sadasivam Karthik, Vishal Changrani, T. Andrew Yang. “Scenario Based Performance Evaluation of Secure Routing in MANETs”. http://sce.uhcl.edu/sadasivamk/MANETII05-draft.pdf
5. Josh Broch, David A. Maltz, David B. Johnson, Yih-Chun Hu and Jorjeta Jetcheva. “A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols”. IEEE Journal on Selected Areas in Communication, 1999. http://monarch.cs.rice.edu/monarch-papers/mobicom98.pdf
6. Yuxia Lin, A. Hamed Mohsenian Rad, Vincent W.S. Wong, and Joo-Han Song. “Experimental Comparisons between SAODV and AODV Routing Protocols”. In proceedings of the 1st ACM workshop on Wireless multimedia, 2005. http://www.ece.ubc.ca/~vincentw/C/LRWSc05.pdf
7. Samir R. Das, Charles E. Perkins, Elizabeth M. Royer. “Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks”. Proceedings IEEE Infocom page 3-12, March 2000. http://www.cs.ucsb.edu/~ebelding/txt/Perkins_Perf Comp.pdf
8. D B. Johnson, D A. Maltz, and Y. Hu. “The dynamic source routing protocol for mobile ad hoc network,", Internet-Draft, April 2003. http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt
9. C.E. Perkins, E. Royer, and S.R. Das. “Ad hoc on demand distance vector (AODV) routing", Internet Draft, March 2000. http://www.ietf.org/internetdrafts /draft-ietf-manet-aodv-05.txt
10. C.Siva Ram Murthy and B. S. Manoj. “Ad hoc wireless networks: Architecture and Protocols”. Prentice Hall Publishers, May 2004, ISBN 013147023X.
11. C.-K. Toh. “Ad Hoc Mobile Wireless Networks: Protocols and Systems”. Prentice Hall publishers, December 2001, ISBN 0130078174.
12. David B. Johnson David A. Maltz Josh Broch. “DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks’.In Ad Hoc Networking, edited by Charles E. Perkins, Chapter 5, pp. 139-172, Addison-Wesley, 2001. http://www.cs.ust.hk/~qianzh/COMP680H/reading-list/johnson01.pdf
13. M. Marina and S. Das. “Performance or Route caching strategies in Dynamic Source Routing”. Proceedings of the Int'l Workshop on Wireless Networks and Mobile Computing (WNMC) in conjunction with Int'l Conf. on Distributed Computing Systems (ICDCS), Washington, DC, USA, 2001. http://www.cs.utsa.edu/faculty/boppana/papers/phd-tdyer-dec02.pdf
14. Charles E. Perkins and Elizabeth M. Royer. ”Ad hoc on demand Distance vector routing”. Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, February 1999, pp. 90-100. http://wisl.ece.cornell.edu/ECE794/Mar5/perkins-aodv.pdf
15. William Stallings. “Network Security essentials: Application and Standards”, Pearson Education, Inc 2003, ISBN 0130351288.