ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 9, November 2012

Simulation analysis of secure routing in Mobile Ad hoc networks

Shawkat K. Guirguis[1], Youssef A. Othman[2]

Professor of Computer Science & Informatics Dept. of Information Technology
Institute of Graduate Studies & Research, Alexandria University, Alexandria, Egypt[1]
Researcher in Dept. of Information Technology
Institute of Graduate Studies & Research, Alexandria University, Alexandria, Egypt[2]

ABSTRACT*: Mobile ad-hoc networks (MANETs) is an appealing technology that has attracted lots of research efforts over past years. Although the principle of wireless, structure-less, dynamic networks is attractive, there are still some major flaws that prevent commercial expansion. Security is one of these main barriers; MANETs are known to be particularly vulnerable to security attack. In this paper we discuss the secure routing in MANETs and evaluate the performance and security of the some secure protocol of MANETs, ns-2 simulations are performed to evaluate the impact of Mobility of the different number of nodes also malicious threats and attacks in the simulation environments .*

Keywords: **security, Ariadne, SRP, SOLSR, SAODV,MANET**

I. INTRODUCTION

MANETs[1] introduce a communication paradigm, which does not require a fixed infrastructure, they rely on wireless terminals for routing and transport services. The network topology of such a system is changeable and unpredictable; therefore, the traditional wired network routing protocols are not applicable for these networks. The special features of a MANET bring about great opportunities together with severe challenges. Due to their highly dynamic topology, the absence of an established infrastructure for centralized administration, bandwidth constrained wireless links, and limited resources, the security requirements (availability, confidentiality, integrity, authentication, nonrepudiation)[2] remain the same whether be it the fixed networks or MANETs the MANETs are more susceptible to security attacks [3] than fixed networks due their inherent characteristics[4]. Securing the routing process is a particular challenge due to open exposure of wireless channels and nodes to attackers. In this paper, we review the main security issues and existing solutions in MANET, and discuss the performance and security of four formal proposed secure routing protocols .

II. SECURITY ASPECTS OF MANETS

MANETs require the four standard security attributes [5].

• *Availability*, which requires that the system stays up and in a working state, and provides the right access and functionality to each user. This security aspect is the target of DoS or DDoS attacks.

• *Confidentiality***,** which requires that the information will not be read or copied

by unauthorized parties. Authentication and other access control techniques are used to achieve this goal.

• *Authenticity*, which requires that the communication peer is really the legitimate node and is exactly whom we expect to talk to, and that the content of a message is valid.

• *Integrity*, which requires that communication data between nodes must not be modified by any unauthorized, unanticipated or unintentional parties.

III. SECURITY CHALLENGES

A central vulnerability of MANET comes from Peer-to-Peer architecture in which each node acts like a router to forward packets to other nodes. Moreover, these nodes on network share the same opened environment that gives opportunity for malicious attackers. In [6] and [7], the challenges for MANET security can be summarized as follows:

• **Lacking of central points**: because of characteristics of MANET such lacking gateways, routers, etc, the mobile nodes just know some neighbours in its range. This introduces new difficulties for security designs such as facing with the change of network topology, resource constraint .

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 9, November 2012

• **Mobility**: MANET nodes can leave, join, and roam in the network on their own will, so the topology of network is changed frequently . Therefore, some proposed security solutions to adapted with the change of topology. However, this also raises new problems for these systems.

• **Wireless link**: In wireless environment, a plenty of collision occurred when nodes send and receive the packets. The wireless channel is also subject to interferences and errors, exhibiting volatile characteristics in terms of bandwidth and delay. In addition, some services such as routing protocols, broadcast services have to communicate with others in real-time, this can flood the network traffic.

• **Limited resources**: The mobile nodes like laptop, PDA are generally constraint in battery power, processing speed, storage, and memory capacity. Therefore, the operation of security solutions can be reduced the accuracy, efficiency such dropping packets, a numerous time for computation.

• **Cooperativeness**: MANET is a mobility network, so nodes have to communicate with others by using routing protocol such AODV, DSR…Therefore, this can make these protocols to become a target of the attacks .

IV. THREATS IN MOBILE AD HOC NETWORKS

the Protocols in MANET are vulnerable to many different types of attacks. In this section, I would like to list different types of attacks that are possible in these networks[8].

Attacks Using Modification An attacker node may modify certain contents of the routing packet, thus propagating incorrect information in the network

Attacks Using Impersonation A malicious node may try to impersonate a node and send data on its behalf. This attack is generally used in combination with modification attack.

Attacks Using Fabrication An attacker may try to fabricate a false Route Error message, which may cause other nodes to remove a particular node from it routing table.

Black Hole An attacker may create a routing black hole, in which all packets are dropped. by sending forged routing packets, the attacker could route all packets for some destination to itself and then discard them.

Gray Hole As a special case of a black hole, an attacker could create a gray hole, in which it selectively drops some packets but not others, for example, forwarding routing packets but not data packets

Replay In replay attack, previously captured routing traffic is sent back into the network to target new routes.

Wormhole This attack requires two malicious nodes where one node captures routing traffic, and sends it to the other malicious node. Then, the second node can send back selective information to the network.

Blackmail Here, the attacker can fabricate a list to block nodes and inject it into the network. This attack targets routing protocols that block malicious nodes by sending a black list of offenders to legitimate nodes.

Denial of Service This attack has two types: a) Routing table overflow, and b) Sleep deprivation torture. In the first type, the attacker floods the network with bogus route creation packets in order to prevent the correct creation of routing information, and to consume resources of nodes. In Sleep deprivation torture, the attacker sends diverse routing information to a specific node in order to make it consume its batteries because of the constant routing processing.

V. ISSUE IN SECURING THE ROUTING PROTOCOLS

Securing the routing protocols for ad hoc networks is a very challenging task due its unique characteristics [9]. A brief discussion on how the characteristics causes difficulty in providing security in ad hoc wireless network is given below.

Shared radio channel: Unlike the wired networks where a separate dedicated transmission line can be provided between a pair of end users, the radio channel used for communication in ad hoc networks is broadcast in nature and shared by all nodes in the network. Data transmitted by a node is received by all the nodes within its direct transmission range. So a malicious node can easily obtain data being transmitted in the network.

Insecure environment: The environment in which MANET are generally used may not be always secure, for example, a battle field. In such environment, nodes may move in and out of hostile and insecure enemy territory, where they would be highly vulnerable to security attacks.

Lack of central authority: In wired networks or infrastructure based wireless networks it would be possible to monitor the network traffic through routers or base stations and implement security mechanisms at those points. Since MANET don't have any such central points, these mechanisms can't be applicable to them.

Lack of association rules: In MANET, since nodes can leave or join the network at any point of time, if no proper authentication mechanism is used for associating nodes with the network intruders can easily join the network and carry out attacks.

Limited availability of resources: Resources such as bandwidth, battery power and computational power are scare in ad hoc networks. Hence, it is difficult to implement complex cryptography-based security mechanisms in such networks.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 9, November 2012

VI. CRYPTOGRAHIC MECHANISM FOR ROUTING IN MOBILE AD HOC NETWORKS

Cryptographic mechanism [10] is the most common and reliable means to ensure security and is not specific to *ad hoc* wireless networks, but can be applied to any communication network. This is some of the main mechanism used in MANETs :

-
-
-

A. *Asymmetric cryptography :*

It is also known as public-key cryptography. In public key cryptography, there is a pair of public/private keys. The private key is kept private, while the public key can be public to others. One of the earliest public-key cryptographic techniques, known as RSA, was developed in the 1970s. Since the 1970s, a large number of encryption, digital signature, key management, and other techniques have been developed in public-key cryptography, such as the ElGamal cryptograph system, DSA, and elliptic curve cryptography.

B. *Symmetric cryptography:*

The encryption key is closely related to the decryption key in that they are identical in most cases. In practice, keys represent a shared secret between two or more parties that can be used to maintain private communication. Usually the network can choose a shared secret key to encrypt and decrypt the message once two more parties use a public/private key pair to build trust in the hand-shake stages, which is more feasible and efficient from a computational standpoint than asymmetric key techniques.

C. *HMAC message authentication code:*

It is a type of message authentication code calculated using a hash function in combination with a secret key. It can also be used to make sure that the message sent unencrypted retains its original content by calculating the message HMAC using a secret key.

D. *Hash chain:*

It is generated by a successive application of a hash function to a string. In [11] the authors suggested the use of hash chains as a password protection scheme. Due to the one-way property of secure hash functions, it is impossible to reverse the hash function. The hash chain length is set to a limited number, and it is used as a reversed order of generation. For example, SAODV and ARIADNE are applications in MANETs that use one-way key chains.

VII. SECURE ROUTING PROTOCOLS

A. *Ariadne*

Ariadne is a secure on-demand routing protocol that protects against node compromise and relies on highly efficient symmetric cryptography [11] .

It discovers route on demand and the concept is primarily based on DSR. Ariadne can authenticate routing messages in the following ways:

shared secret between each pair of nodes,

shared secret between communicating nodes combined with broadcast authentication .

using digital signature.

In Ariadne with digital signature not only the source and destination nodes authenticate the messages, but also the intermediate nodes insert their own digital signatures in route requests. In addition, Ariadne uses per-hop hashing to prevent removal of identifiers from the list of routes in the route request. Ariadne with TESLA [12] is an efficient broadcast authentication scheme that requires loose time synchronization. Use of pair wise shared keys can avoid the need for time synchronization but it costs a higher keysetup overhead. However, it does not elaborate the solution for key agreement to establish the pre-shared secret key between the source and destination nodes.

Ariadne makes use of symmetric key cryptography. It also uses a one way hash along with a MAC using a shared key between the source and the destination in order to authenticate the source at the destination. Every intermediate node on a particular route adds, along with its address, its own message authentication code. As a result, the source node can authenticate all individual entries in the route reply path.

The basic operation of the protocol can be summarized as follows:

A route request packet is sent out by the initiator when communication is to be commenced. The RREQ has information such as an identifier for the particular route that has been discovered along with a TESLA time interval.

Upon receipt of the RREQ, the recipient intermediate node checks whether the TESLA time interval is still valid.

The hash function described earlier is used to check the authentication. Each hop on the path is verified by the target node by comparing the computed hash and the received hash [13].

B. *SAODV*

A secure version of AODV [14]called Secure AODV (SAODV)it proposed in [15].

It provides features such as integrity, authentication, and non-repudiation of routing data. It incorporates two schemes for securing AODV. To preserve the collaboration mechanism of AODV, SAODV includes a kind of delegation feature that allows intermediate nodes

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 9, November 2012

to reply to RREQ messages. This is called the *double signature*: when a node A generates a RREQ message, in addition to the regular signature, it can include a second signature, which is computed on a fictitious RREP message towards A itself. Intermediate nodes can store this second signature in their routing table, along with other routing information related to node A. If one of these nodes then receives a RREQ towards node A, it can reply on behalf of A with a RREP message, similarly to what happens with regular AODV. To do so, the intermediate node generates the RREP message, includes the signature of node A that it previously cached, and signs the message with its own private key.

SAODV does not require additional messages with respect to AODV. Nevertheless, SAODV messages are significantly bigger, mostly because of digital signatures. Moreover, SAODV requires heavyweight asymmetric cryptographic operations: every time a node generates a routing message, it must generate a signature, and every time it receives a routing message (also as an intermediate node), it must verify a signature. This gets worse when the double signature mechanism is used, because this may require the generation or verification of two signatures for a single message. In the SAODV operations, SAODV allows to authenticate the AODV routing data. Two mechanisms are used to achieve this: hash chains and signatures[16].

C. *SRP*

SRP [18] is another protocol extension that can be applied to many of the on demand routing protocols used today. SRP defends against attacks that disrupt the route discovery process and guarantees to identify the correct topological information. The basic idea of SRP is to set up a security association (SA) between a source and a destination node without the need of cryptographic validation of the communication data by the intermediate nodes. SRP assumes that this SA can be achieved through a shared key KST between the source S and target T . Such a security association should exist prior to the route initiation phase. The source S initiates the route discovery by sending a route request packet to the destination T . The SRP uses an additional header called SRP header to the underlying routing protocol (e.g., AODV) packet. SRP header contains the following fields: the query sequence number Q*SEC*, query identifier number Q*ID*, and a 96 bit MAC field.

Intermediate nodes discard a route request message if SRP header is missing. Otherwise, they forward the request toward destination after extracting Q*ID*, source, and destination address. Highest priority is given to nodes that generate requests at the lowest rates and vice versa. When the target T receives this request packet, it verifies if the packet has originated from the node with which it has SA. If Q*SEC* is greater or equal to Q*MAX*, the request is dropped as it is considered to be replayed. Otherwise, it calculates the keyed hash of the request fields, and if the output matches SRP MAC, then authenticity

of the sender and integrity of the request are verified.

On the reception of a route reply, S checks the source address, destination addresses, Q*ID*, and Q*SEC*. It discards the route reply if it does not match the currently pending query. In case of a match, it compares reply IP source-route with the exact reverse of the route carried in reply packet. If the two routes match, then S calculates the MAC by using the replied route, the SRP header fields, and the secure key between source and destination. If the two MAC match, then the validation is successful, and it confirms that the reply did came from the destination T .

SRP suffers from the lack of validation mechanism for route maintenance messages as it does not stop a malicious node from harming routes to which that node already belongs to. SRP is immune to IP spoofing because it secures the binding of the MAC and IP address of the nodes, but it is prone to wormhole attacks and invisible node attacks.

D. *SOLSR*

Secure Optimized Link State Routing Protocol proposed by Amanpreet Kaur, Gurpreet Deol [18] it based in Optimized Link State Routing Protocol [19] , provide the security with the help of signature scheme. And the approach provides the authentication between the two nodes. For providing the signature the approach use the two functions. First one is for signature and the second is for verification

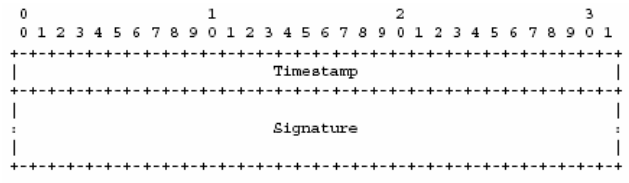
1. Sign (node *id*, key, message) A signature for a message can be verified in a node using a function:
2. Verify (originator id, key, message, signature).

To prevent malicious nodes from injecting incorrect information into the OLSR network, the originator of each control generates an additional security element called signature message and transmitted with the control message. A timestamp is associated with each signature in order to estimate message freshness. Thus, upon receiving the control message, a node can determine if the message originates from a trusted node, or if message integrity is preserved. Signatures are separate entities from OLSR control traffic: while OLSR control messages perform the purpose of acquiring and distributing topological information, signatures serve to validate information origin or integrity.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 9, November 2012

The SIGNATURE message is encapsulated and transmitted as the data portion of the standard OLSR packet format.



The Timestamp field contains the timestamp itself, measured in seconds. This is the timestamp of both the SIGNATURE message and the associated control message.

Timestamps are a commonly used means to prevent replay attacks. They provide the proof of newness so that older pieces of information can be detected and rejected. The criterion to verify whether a timestamp is old is:

$$| \text{Timestamp} - t_0 | \leq \Delta t$$

where t_0 is the current time at the receiving node and Δt is the accepted value for discrepancy, including the difference in the synchronization of clocks.

To compute a signature corresponding to a control message, the following protocol is used:

1. the node creates the control message;
2. the node retrieves the current time, and writes it in the Timestamp field;
3. the node computes the signature, and writes it in the Signature field;
4. the node puts the SIGNATURE message and the control message in the packet, in this exact order.

Then, the node sends the packet, or repeats the protocol for another control message before sending the packet.

Upon receiving a control message with its SIGNATURE message, a node processes both. The outline of protocol is given below:

1. the node processes the SIGNATURE message, checking the timestamp, and keeps the SIGNATURE in memory;
2. the node checks the signature of the control message;
3. if the timestamp is fresh and the signature is valid, the control message is accepted and processed according to the standard OLSR specifications for the message type. If not, both the control message and SIGNATURE message are dropped.

VIII. METHODOLOGY OF EVALUATION

In our evaluation, we compare the performances of Ariadne ,SAODV , SRP and SOLSR using Network Simulator 2.34 (NS-2) [20]. The details of simulation environment and the performance metrics are given in the following subsections.

E. Simulation Environment

At the physical and data link layer, we used the IEEE 802.11 with Two Ray Ground radio propagation model. We have considered the traffic of Constant Bit Rate (CBR) data packets over UDP. Table 1 summarizes the complete setup for the simulation.

TABLE I

SIMULATION SETUP

Parameter	Value
Simulation tool	NS-2 (2.34)
Area Size	1000 m * 1000 m
Maximum Speed	20 m/s
Maximum Connection	20
Packets Rate	4 Packets / Second
Traffic Type	CBR over UDP
Simulation Time	600 (sec)
Pause Time	0,100,200,300,400,500,600
Packet Size	512 bytes
Number of node	50,100,150,200,250
Malicious nodes	5,10,15,20,25

F. Performance evaluating metrics :

In order to evaluate the performance of the concerned secure routing protocols, the following five metrics are considered:

Packet Delivery Fraction (PDF): This is the ratio of the number of data packets successfully delivered to the destinations to those generated by sources.

Normalized Routing Load (NRL): The number of routed packets transmitted per data packet delivered at the destination.

Average End-to-End Delay (AED): It is defined as the average time taken by data packets to propagate from source to destination across the network. This includes all possible delays under Pause time and nodes also in malicious node.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 9, November 2012

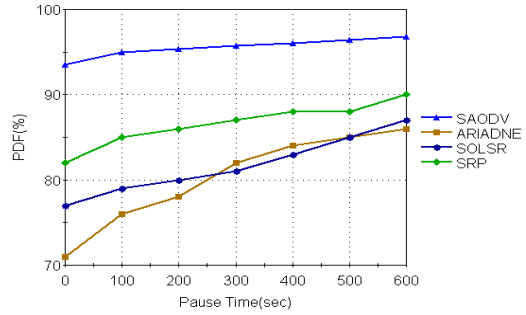


Fig. 1 PDF (%) vs Pause Time

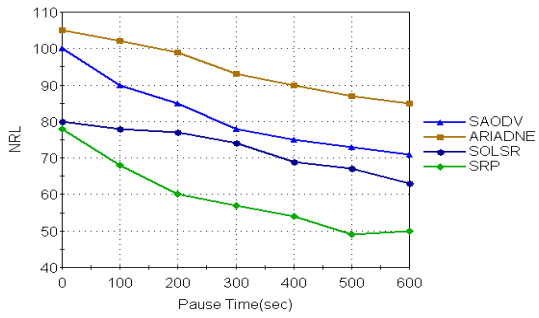


Fig. 2 NRL vs Pause Time

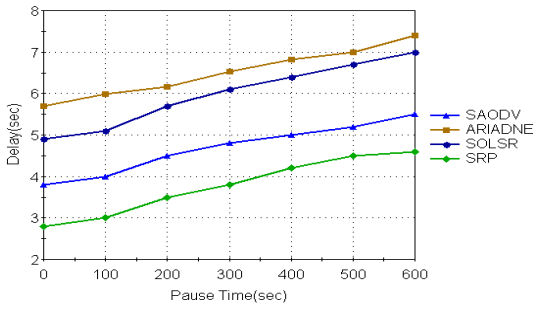


Fig. 3 AED vs Pause time

1) The impact of variation in pause time :

In figure 1, SAODV shows higher PDFs about in average 95% and SRP shows percentage 86.5% SOLSR about 81,7% and the lowest one is Ariadne with average 80.28% . We observe that in small pause time the protocol gives lowest PDFs and for higher pause times , the protocols converge to give a large PDFs because the nodes are almost static and hence the congestion in the network decreases.

In figure 2, Ariadne shows high NRL (due to the authentication overhead in Route Request, Reply and Error) and also SAODV because it relay on asymmetric cryptography and SOLSR show less NRL by 20 % and the lowest NRL is SRP. The NRL reduce in large pause time (less mobility).

The results from figure 3, shows Ariadne gives large delay because the TESLA (Timed Efficient Stream Loss-Tolerant Authentication) broadcast protocol and time synchronization. and second large delay is SOLSR And then SAODV and the smallest delay it achieve by SRP .

In low pause time the protocols achieve minimum delay because high mobility of the nodes .

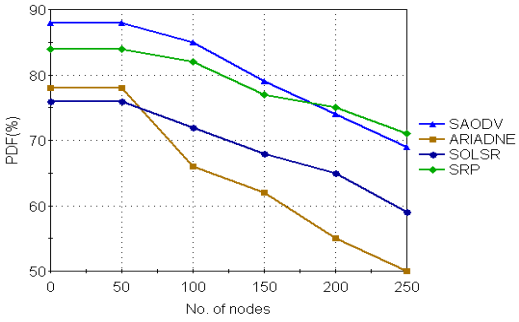


Fig. 4 PDF vs No. of nodes

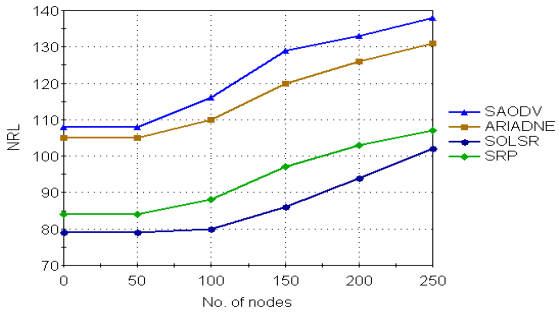


Fig. 5 NRL vs No. of nodes

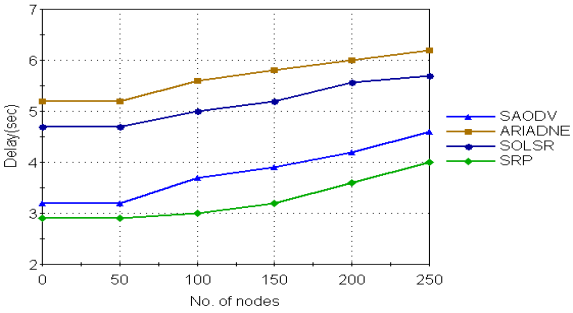


Fig. 6 Delay vs No. of nodes

2) The impact of variation in number of nodes :

In figure 4, with fixed pause time and increasing the number of nodes the PDFs decrease. SAODV shows highest PDFs percentage 88% in 50 nodes and SRP start with 84% and in 250 node give higher PDFs than SAODV, Ariadne in 50 node show 78% but in large number of node show the lowest performances.

The figure 5, shows SAODV gives highest NRL due to asymmetric key use to encrypt the packets . and the

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 9, November 2012

Ariadne shows high load but less than SAODV and then SRP, and SOLSR gives the minimum load due to from flooding of control traffic by using only selected nodes, called MPRs (Multi Point Relays) . The NRL is increase with increasing the number of nodes

The results in figure 6, shows Ariadne had larger time delay (because in Ariadne all nodes in networks should be time synchronized), and then SAODV it requires significant processing time to compute or verify signatures and hashes at each node. the OLSR and SRP relatively show low delay.

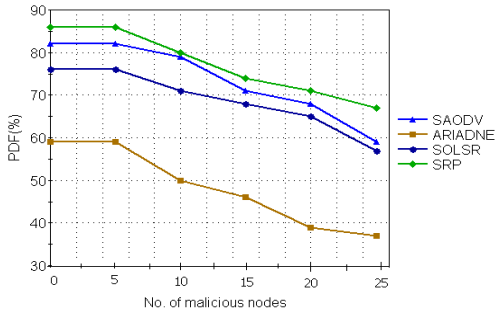


Fig. 7 PDF vs No. of malicious nodes

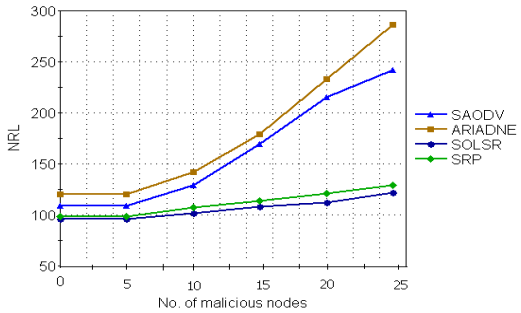


Fig 8. NRL vs No. of malicious nodes

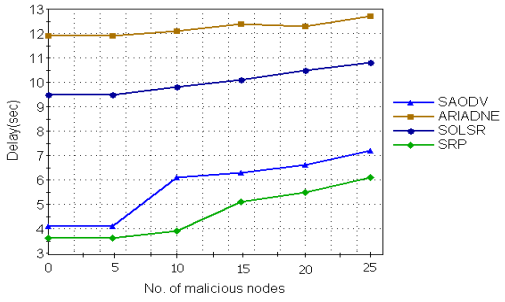


Fig . 9 Delay vs No. of malicious nodes

3) Impact of malicious nodes :

In figure 7, PDFs actually Decreases when the number of malicious node increases (due to decrease the number of routing packets). Ariadne gives the lowest PDFs by average percentage 46.2% and then the SOLSR with average value 68% after that SAODV and the best performance by SRP.

In figure 8,The NRL increase with increasing the malicious node (due to extra routing communications needed to handle the malicious nodes). Ariadne shows highest NRL (because the hard and complex secure mechanism) next high load is showing is SAODV, the NRL in SRP and SOLSR slightly close to each other.

From result showing in figure 9,time delay increases with increase in malicious nodes because in the presence of malicious nodes, more time is required to deliver data packet to destination node, Ariadne shows large delay and the lowest delay in the above graph is SRP.

IX. CONCLUSION

In mobile ad-hoc networks, an attacker can easily disrupt the functioning of the network by attacking the underlying routing protocol. Hence, security in ad hoc networks is still a debatable area. In this paper, Analytical study has been carried out for existing secure routing protocols for wireless mobile ad hoc networks, this study include simulation analysis of these protocols and the impact of mobility and the number of the nodes in mobile ad hoc networks, also the impact of malicious environments and how each protocol react to the malicious node. We believe that more work is still required to justify the exact definition for secure ad hoc routing which will allow researchers to formally prove whether a proposed protocol satisfies all the security issues concerning Ad hoc Networks.

REFERENCES

[1] C.S.R.Murthy and B.S.Manoj, Ad Hoc Wireless Networks, Pearson Education, 2008.

[2] A.Weimerskirch and G.Thonet, "Distributed Light-Weight Authentication Model for Ad-hoc Networks," *Lecture Notes In Computer Science*; Vol. 2288, pp. 341-354, 2001.

[3] Kejun Liu, Jing Deng, Member, Pramod K. Varshney, Fellow, Kashyap Balakrishnan, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs" IEEE Transaction on Mobile Computing, VOL. 6, NO. 5, May 2007.

[4] I.Chlamtac, M.Conti, and J.Liu, "Mobile Ad Hoc Networking: Imperatives and Challenges," *Ad Hoc Networks*, vol. 1, no. 1, pp. 13- 64, 2003.

[5] Eric Lee , Security in Wireless Ad Hoc Networks , Science Academy Publisher, United Kingdom , Vol. 1, No. 1, March 2011.

[6] Celia Li1, Zhuang Wang, Cungang Yang ,Secure Routing for Wireless Mesh Networks , International Journal of Network Security, Vol.12, No.3, May 2011

[7] J.Viji Gripsy , Dr. Anna Saro Vijendran ,A Survey on Security Analysis of Routing Protocols Global Journals Inc. (USA) , Volume 11 Issue Version 1.0 April 2011

[8] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Rushing attacks and defense in wireless ad hoc network routing protocols. In Proceedings of the 2003 ACM Workshop on Wireless Security, pages 30–40, ACM Press, 2003.

[9] Ashwani Kumar, A survey on routing protocols for wireless sensor networks , IJAER , Vol.No.I, Issue No.2, February 2011

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 9, November 2012

[10] A. Menezes, P. Van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.

[11] Secure Hash Signature Standard (SHS). Technical Report FIPS PUB 180-2, NIST, August 1 2002.

[12] Y.C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," *Proceedings of the 8th Annual International Conference Mobile Computing and Networking (MobiCom 2002)*, ACM Press, 2002, pp.12-23.

[13] Adrian Perrig, Ran Canetti, Doug Tygar, and Dawn Song. Efficient authentication and signature of multicast streams over lossy channels. In Proceedings of the IEEE Symposium on Research in Security and Privacy (S & P 2000), pages 56–73, May 14–17 2000.

[14] A. Perrig, R. Canetti, J.D. Tygar, and D. Song. Efficient authentication and signing of multicast streams over lossy channels. *In proceedings of the IEEE Symposium on research in Security and Privacy*, May 2000.

[15] Perkins C, Royer E. Ad hoc on-demand distance vector routing. Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, February 1999.

[16] M. Guerrero Zapata and N. Asokan, Securing Ad hoc Routing Protocols, in Proceedings of the 1st ACM workshop on Wireless security, Sep 2002.

[17] G.S. Mamatha and Dr. S. C. Sharma, "A Highly Secured Approach against Attacks in", International Journal of Computer Theory and Engineering, Vol. 2, No. 5, October, 2010.

[18] P. Papadimitratos and Z. J. Haas, Secure Routing for Mobile Ad hoc Networks, In Proc. of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), Jan. 2002.

[19] Cédric Adjih, Thomas Clausen, Philippe Jacquet, Anis Laouiti, Paul Mühlethaler, and Daniele Raffo. Securing the OLSR protocol. In Proceedings of the 2nd IFIP Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net 2003), Mahdia, Tunisia, June 25–27 2003.

[20] The Network Simulator NS-2 tutorial homepage, http://www.isi.edu/nsnam/ns/tutorial/index.html