Implementation of New Routing Protocol for Node Security in a Mobile Ad Hoc Network

Virendra Singh Kushwah kushwah.virendra248@gmail.com
Department of Computer Science
Hindustan Institute of Management and
Computer Studies,
Farah, Mathura, INDIA

Gaurav Sharma gauravsharma53@gmail.com
Department of Computer Science
GLA University,
Mathura, INDIA

Abstract

A routing protocol plays important role to handle entire network for communication and determines the paths of packets. A node is a part of the defined network for transferring information in form of packets. If all packets transferred from source to destination successfully, it has been assumed that the routing protocol is good. But, an attacker turns this dealing as a speed breaker and turning point of a highway. So, prevention from attacks and secure packets, a new routing protocol is being introduced in this paper. The proposed routing protocol is called by SNAODV (Secure Node AODV). This paper is also tried to maximize throughput as compared with AODV and SAODV.

Keywords: AODV, Routing, Secure, Packets, Network.

1. INTRODUCTION

A mobile ad hoc network (MANET) consists of a group of devices (or nodes) that rely on the wireless communication medium and themselves for data transmission. A node in an ad hoc network has direct connection with a set of nodes, called neighbouring nodes, which are in its communication range. The number of nodes in the network is not necessarily fixed. A MANET does not have base stations or routers. Each node acts as a router and is responsible for dynamically discovering other nodes it can directly communicate with. However, when a message without encryption is sent out through a general tunnel, it may be maliciously attacked. Nodes cooperate by forwarding packets on behalf of each other when destinations are out of their direct wireless transmission range. A centralized administrator and/or a pre-deployed network infrastructure are not necessary for a MANET to be set up, thus making its deployment quick and inexpensive.

In addition, Nodes ability to move freely ensures a flexible and versatile dynamic network topology which can be desirable in many situations. Hence, in addition to acting as hosts, each mobile node does the functioning of routing and relaying messages for other mobile nodes. Being mobile, any node can communicate to other nodes. Nodes do not necessarily know each other and come together to form an ad hoc group for some specific purpose. While limited bandwidth, memory, processing capabilities and open medium make its disadvantages. There are two types of possible attacks on nodes in MANET: passive attacks and active attacks. In passive attacks, adversaries simply drop and refuse to forward other nodes requests of assigning keys. In active attacks, in contrast, adversaries may return a fake reply (e.g. an invalid partial key) to the node requesting key. However, the security of MANET is still a challenge issue.

2. PROBLEM STATEMENT

There are a number of solutions for securing routing protocols in MANETs. We know there are two authentication models for securing routing is available that are ARAN [14] and SAODV [15] since they are closely related to our proposed model. In general, the existing schemas/models for secure routing are based on the assumptions of the availability of key management infrastructures which are unrealistic and contrast to the ad hoc network concepts. Moreover, these schemas do not consider intermediate nodes during the routing steps; therefore, the nodes may perform fabrication attacks. From these weaknesses of current approaches, our goal is to design a schema which performs point-to-point message authentication without a deployed key management infrastructure.

When two nodes are communicating, there may be any chance to steal packets, destroy packets or corrupt packets by malicious nodes. There are following two questions:-

1. Are nodes making right communication?
2. Are packets being saved during transmissions?

If these two questions are solved, at least it is understandable to prevent from misbehaviour nodes which make interfered between two or more right nodes during transmission of packets. So prevention is better than cure. To detect malicious nodes and remove those nodes is two way process [2]. So follow two processes, it is better process to use certificate on those nodes. If those nodes are secured, at least packets can be saved from attackers during transmission.

3. LITERATURES REVIEW

Security has become wide research area in MANETs. Most existing papers on deploying key management in MANETs usually mention flooding briefly as a way to distribute key in an ad hoc network using AODV routing protocol. Most secure communication protocols rely on a secure, robust and efficient key management scheme. Key management is also a central aspect for security in mobile ad hoc networks. In mobile ad hoc networks, the computational load and complexity for key management are strongly subject to restriction by the node's available resources and the dynamic nature of network topology.

1. A secure identity based key management scheme is proposed suitable for applying in MANETs. Similar to other ID-based cryptosystems, a trusted key generation center is needed in this scheme for verifying user identity and generating the corresponding private keys. [4]

2. Research work in key management scheme and handlings about limited number of nodes are possible in an ad hoc network. When the number of nodes increases, most of them become either inefficient or insecure. The main problem of any public key based security system is to make user's public key available to others in such a way that is authencity is verifiable. [5]

3. Using novel hierarchical security scheme, called Autonomous Key Management (AKM), which can achieve flexibility and adaptivity, and handles MANET with a large number of nodes. AKM is based on the hierarchical structure and secret sharing to distribute cryptographic keys and provide certification services. AKM also enables the ability to issue certificates with different levels of assurance with the help of a relatively small number of nodes. [6]

4. SEKM (Secure and Efficient Key Management) builds a public key infrastructure (PKI) by applying a secret sharing scheme and using an underlying multicast server groups. In SEKM, each server group creates a view of the certificate authority (CA) and provides certificate update service for all nodes, including the servers themselves. The advantage is that in SEKM it is easier for a node to request service from a well maintained group rather than from multiple "independent" service providers which may be spread in a whole area. [7]

5. In Authenticated Acknowledgement Scheme (AAS) to detect such selfish nodes, routes containing such nodes will be eliminated from consideration. The source node will be able to choose an appropriate route to send its data. The AAS scheme is a network-layer technique to detect the selfish nodes and to mitigate their effects. It can be implemented as an add-on to existing routing protocols for MANETs, such as DSR. The AAS scheme detects misbehavior through the use of a new type of authenticated acknowledgment scheme termed AAS, which assigns a fixed route of two hops (three nodes) in the opposite direction of the data traffic route. When a node wishes to communicate with another node, a methodology is performed by the sending and receiving nodes, which ensures authentication and integrity. [8]

6. In [14], the authors categorized three kinds of threats which are modification, impersonation and fabrication in AODV and DSR. On the basic of this analysis, the authors proposed a protocol called ARAN (Authenticated Routing for Ad hoc Networks) using cryptographic certificates to bring authentication, message-integrity and non-repudiation to the route discovery process based on the assumption of existing of a trusted certificate server. It is not appropriate with ad hoc networks because it forms a centralized element. Moreover, in this protocol, because the source node cannot authenticate intermediate nodes in the routing path, intermediate malicious nodes can use error message attacks to networks.

7. In [15], the authors extend the AODV routing protocol to guarantee security based on the approach of key management scheme in which each node must have certificated public keys of all nodes in the network. This work uses two mechanisms to secure the AODV messages: digital signature to authenticate the fixed fields of the messages and hash chains to secure the hop count field. This protocol uses public key distribution approach in the ad hoc network; therefore, it is difficult to deploy and computationally heavy since it requires both asymmetric cryptography and hash chains in exchanging messages. The protocol also did not consider the authentication of intermediate nodes; hence it could not prevent the attack of falsifying error messages in ad hoc networks.

4. SYSTEM MODEL

The principle of our model is that messages in ad hoc network must be authenticated to guarantee the integrity and non-repudiation so that the protocol and nodes can be prevented against several kinds of attacks. Each node in a network has its own a pair of public key *e* and private key *d* following RSA Public-key Crypto-system [13] by self-generation, and each node contains a list of neighbour nodes with records containing the information of a neighbour node including neighbour address, neighbour public key, and a shared secret key. This information is formed after the key agreement between two neighbour nodes to negotiate a pair of keys and a shared secret key. The details of our security schema for AODV are described as the following sections.

A. Key Agreement Process between Neighbor Nodes

A node joining a network requires sending key agreement messages to its neighbours to negotiate a shared secret key. The concept of this process is based on HELLO message in ad-hoc routing protocols. The node broadcasts a message indicating the negotiation request with neighbour nodes:

$$<KEY\_AGREEMENT\_REQ,\ request\_id,\ sender\_address,\ PK_S>$$

On receiving this request, nodes reply a message:

$$<KEY\_AGREEMENT\_REP,\ request\_id,\ sender\_address,\ neighbour\_address,\ PK_N>$$

(Where PK_S and PK_N are the public key of the sender node and replying node, respectively; *request_id* is a sequence number generated by the sender node) to indicate the receiving of the request message and inform that it is ready for the key agreement process. For each received message, the request node (i.e.; node A) creates a new record in its neighbour list. Each record contains filled neighbour address and filled neighbour public key; the other fields of the record are empty. For each new record in the list, the request node (A) negotiates a secret key with the neighbour node (B) by the following steps:

1. Generate a key Ks by using a secure random number generator,
2. Encrypt Ks with PK_B (node B's public key) = encrypt PK_B (Ks),
3. Send an offer message
   <KEY_PASS, encrypt PK_B (Ks)> to B,
4. Wait ACK (acknowledgement) from B and check message integrity to finish the negotiation

When node B receives the key passing message, it decrypts "*encrypt PK_B (Ks)*" by its private key (pB) to get the shared key K. Then, node B sends the ACK message

<KEY_ PASS_ ACK, request_id, $HASH_{Ks}$ (request_id)>

to indicate successful shared secret key negotiation, where $HASH_{Ks}$ *(request_id)* is the hashed message of *request_id* by the shared key *Ks*.

Since RSA algorithm is used in the negotiation, the confidentiality of the shared key is guaranteed between the two nodes. The shared key is used for authenticating messages between two adjacent nodes later in AODV routing protocol. In the case a node does not have a shared key with its neighbour nodes; it cannot participate in routing transactions.

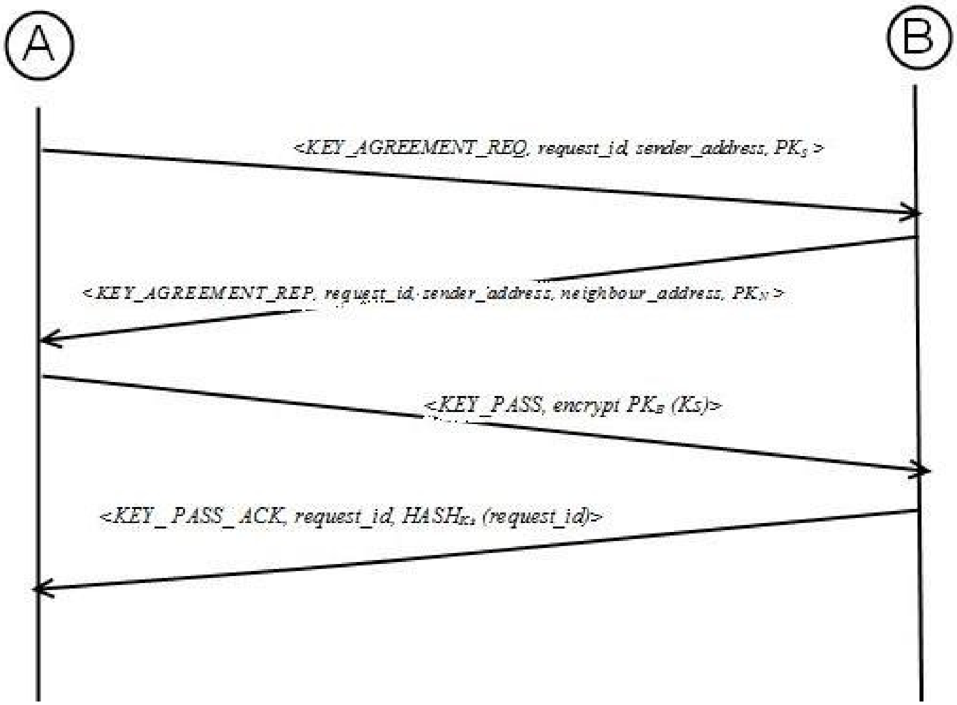


FIGURE 1: Node to node authentication process

B. Route Request

Route request (RREQ) is initiated by a source node (S) and then propagated by intermediate nodes until the message reaches its destination node (D). On receiving RREQ, an intermediate node I, according to our designed routing protocol, checks whether the message will be re-broadcasted or not. If the message needs to be re-broadcasted and the sender is in node I's neighbour list, it will send (unicast) a message to request the authentication process from the sender:

<RREQ_REQ, source_address, broadcast_id>.

When receiving the authentication request, the sender creates an authentication reply message containing

<RREQ_REP, source_address, broadcast_id, HASH$_{Ks}$ (RREQ)>

Where HASH$_{Ks}$ *(RREQ)* is the hashed value of RREQ message by the shared key Ks between the two nodes. The authentication reply message is unicasted back to node I. Node I on receiving the message will check the integrity of the RREQ message by hashing the message with using the shared key Ks and then comparing with the received hashed digest. If the comparison is successful (the integrity of the RREQ message is guaranteed), node I continues steps following AODV such as set up reverse path, increase the hop count, rebroadcast the message and so on; otherwise, the RREQ will be discarded. The process continues until the message reaches the destination. The destination also authenticates the sender of RREQ (neighbour of the destination) by the same procedure.

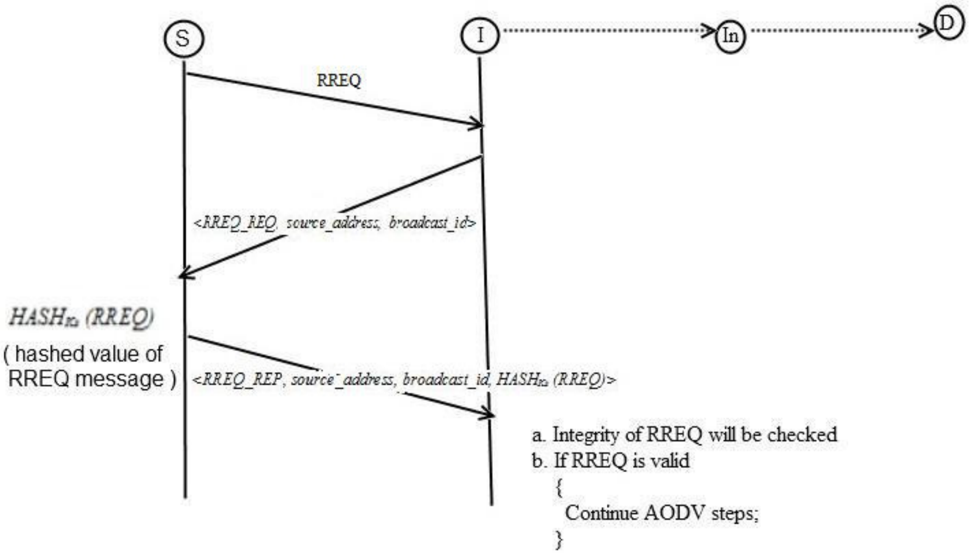

S
I
In
D
RREQ
<RREQ_REQ, source_address, broadcast_id>
HASH$_{Ks}$ (RREQ)
(hashed value of RREQ message)
<RREQ_REP, source'_address, broadcast_id, HASH$_{Ks}$ (RREQ)>
a. Integrity of RREQ will be checked
b. If RREQ is valid
{
Continue AODV steps;
}

FIGURE 2: Representation of the message authentication

C. Route Reply and Route Maintenance

Route replies (RREP) in AODV are also targets for attacks by malicious nodes. In our model, when receiving a RREP, a node requests the sender to proof the integrity and non-repudiation of the message by sending an authentication message. The request for authentication is

<RREP_REQ, destination_address, destination_sequence#>

and the reply is

<RREP_REP, destination_address, destination_sequence#, HASH$_{Ks}$ (RREP)>

where *HASH$_{Ks}$ (RREP)* is the hashed value of RREP message by the shared key Ks between the two nodes. After the authentication process is successful, a node continues to the steps in AODV, otherwise, the node drops RREP since it is invalid.

In route maintenance process, only route error report message (RERR) is a target for attacks in AODV protocol. Our schema requires the authentication process in sending route error messages to prevent attacks from malicious nodes. The authentication request and response for RERR is

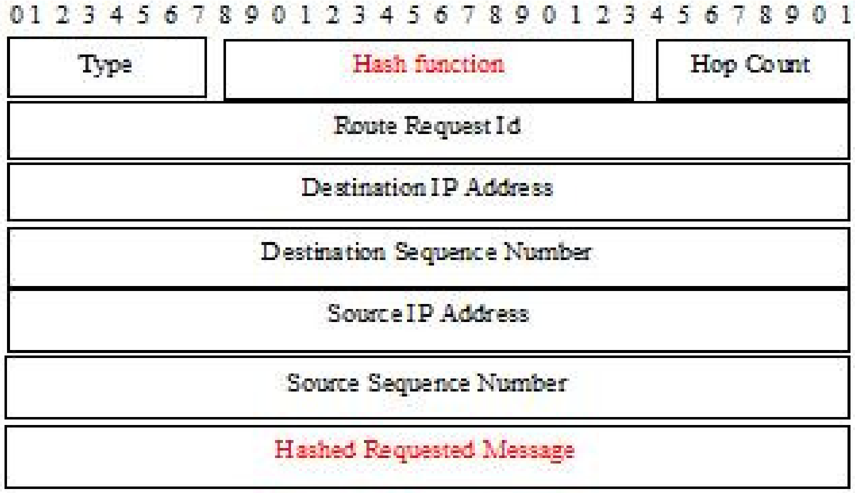
<RERR_REQ, unreachable_destination_address, unreachable_destination_sequence#>,

And

<RERR_REP, unreachable_destination_address, unreachable_destination_sequence#, HASH$_{Ks}$ (RERR)>,

respectively.

D. Routing Message formats



0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Type | Hash function | Hop Count

Route Request Id

Destination IP Address

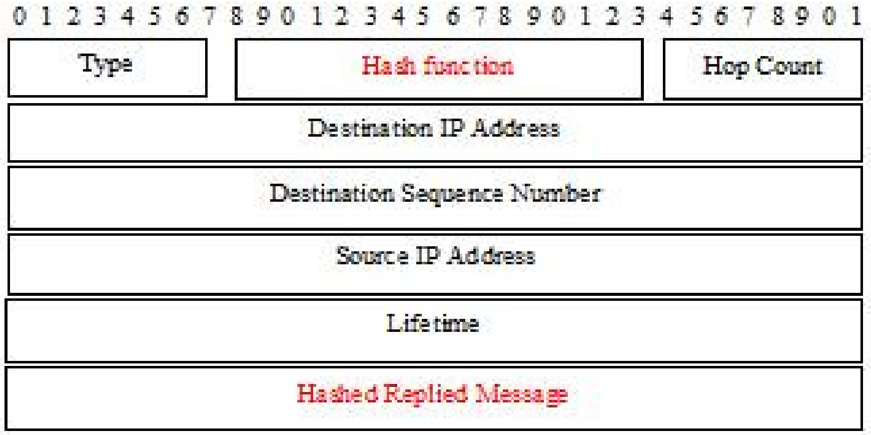
Destination Sequence Number

Source IP Address

Source Sequence Number

Hashed Requested Message

FIGURE 3: RREQ message format of SNAODV



0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Type | Hash function | Hop Count

Destination IP Address

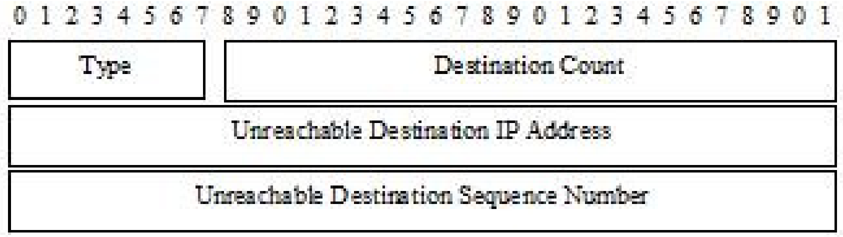
Destination Sequence Number

Source IP Address

Lifetime

Hashed Replied Message

FIGURE 4: RREP message format of SNAODV



0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

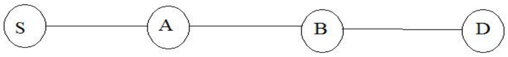
Type | Destination Count

Unreachable Destination IP Address

Unreachable Destination Sequence Number

FIGURE 5: RERR message format of SNAODV

E. Algorithm for node-to-node authentication of the System Model



1. *Sender node broadcasts a message indicating the negotiation request with neighbour nodes*
   <KEY_AGREEMENT_REQ, request_id, sender_address, PK_S >
2. *Sender node gets reply a message*
   <KEY_AGREEMENT_REP, request_id, sender_address, neighbour_address, PK_N >

3. *The request node (A) negotiates a secret key with the neighbour node (B) by the following steps:*
   a. *Generate a key Ks by using a secure random number generator,*
   b. *Encrypt Ks with PK_B (node B's public key) = encrypt PK_B (Ks),*
   c. *Send an offer message*
      <KEY_PASS, encrypt PK_B (Ks)> to B,
   d. *Wait ACK (acknowledgement) from B and check message integrity to finish the negotiation*

4. *Node B sends the ACK message*
   <KEY_ PASS_ ACK, request_id, $HASH_{Ks}$ (request_id)>

5. SIMULATION AND RESULTS

Simulation of the work has been done on QualNet 5.0.1 for implementing new designed routing protocol. We have implemented RREQ and RREP message formats for new routing protocol using hash function i.e.; MD5 (Message Digest 5). It has been given in above figures. Simulation done on the following parameters basis:

Parameters	Value
Simulation Area	1500m x 1500m
Number of nodes	30 (4 nodes are wormhole)
Simulation duration	120 s
Routing protocol	AODV and SNAODV
Mobility pattern of nodes	Random waypoint

TABLE 1: Simulation setup

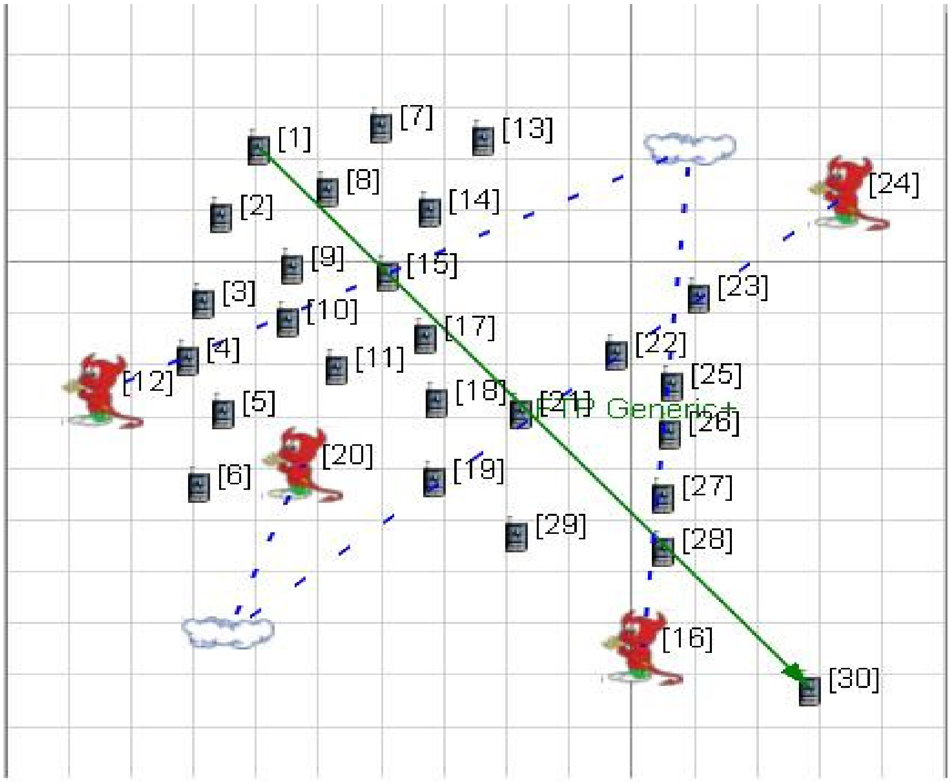


FIGURE 6: 30 nodes MANET environment with 4 blackhole nodes

Parameters	AODV	SNAODV
Throughput	2435	2700
Number of RREQ packets initiated	19	24
Number of data packets sent as source	183	208
Number of data packets received	62	64
Number of RREQ packets retried	30	29
Number of RREQ packets received by dest	19	23
Number of RREP packets initiated as dest	14	20
Number of RREP packets received as Source	15	22

Number of Data Packets Dropped for no route	Node1=31,
	Node2 = 1,
	Node11= 1
		Node1=24,
		Node2 = 11,
		Node11= 0

TABLE 2: Simulation results

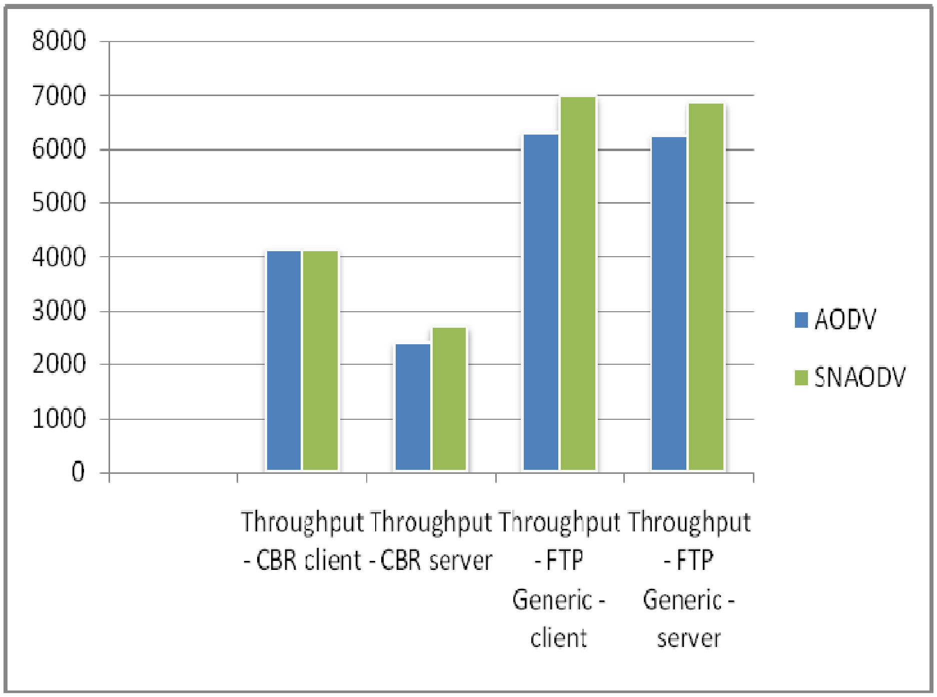


FIGURE 7: Throughput based comparison between AODV & SNAODV

The results have been come out from simulated on Qualnet 5.0 tool on the above simulation parameters and the results are being shown that the goal of new protocol to maximize the throughput. Throughput values of CBR client of both routing protocols are same while throughput values of CBR server is different in our new proposed protocol has higher values than AODV. Same process is in FTP Generic server.

6. CONCLUSION

This paper presents a new secure routing protocol for MANETs. It also provides node to node authentication and enables mobile user to ensure the authenticity of user of peer node. The significant advantage of our solution is to get all packets meaning that packet will be transmitted from source to destination without losing packets. The system model solved the security problem in the ad hoc network and is also suitable for application to other wired and wireless network. This paper is maximizing throughput of the network on the various parameters. One advantage of the SNAODV protocol is that no key assumption is required like SAODV has.

7. REFERENCES

1. L.Zhou and Z.Haas,"Securing AdHoc Networks," IEEE Network, vol.13, no.6, page no.24–30, November/December 1999

2. B. Sukla, "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks", In proceeding of the World Congress on Engineering and Computer Science 2008, October 22-24,2008,San Francisco,USA

3. Nguyen H and Morino H,"A Key Management Scheme for Mobile Ad Hoc Networks Based on Threshold Cryptography for Providing Fast Authentication and Low Signaling Load", IFIP International Federation for Information Processing 2005, LNCS 3823, page no. 905-915,2005

4. A.Kapil and S.Rana, "Identity-Based Key Management in MANETs using Public Key Cryptography", International Journal of Security (IJS), Volume (3): Issue (1), published in Computer Science journal in March, 2009.

5. S. Capkuny, L. Buttyan, J.-P. Hubaux, "Self-organized public-key management for mobile ad hoc networks", Technical Report 2002/34, EPFL/IC, May 2002.

6. Bo. Zhu, Robert H. Deng, Mohan S. Kankanhalli, Guilin Wang, "Efficient and robust key management for large mobile ad hoc networks", In Proceedings of Computer Networks 48 (2005), page no. 657–682, 2005.

7. Bing Wu, Jie Wu, Eduardo B. Fernandez, Mohammad Ilyas, Spyros Magliveras, "Secure and efficient key management in mobile ad hoc networks", Journal of Network and Computer Applications 30 (2007), page no. 937–954, 2007.

8. M. Gunasekaran, P. Sampath and B. Gopalakrishnan, "AAS: An Authenticated Acknowledgement-Based Scheme for Preventing Selfish Nodes in Mobile Ad Hoc Networks", International Journal of Recent Trends in Engineering, Vol 1, No. 1, May 2009, page no. 294-298, 2009.

9. Andreas Hafslund and Jon Andersson, Thales Norway AS, "2-Level Authentication Mechanism in an Internet connected MANET", 6th Scandinavian Workshop on Wireless Ad-hoc Networks, 2006.

10. Marcelo M. Carvalho, Cintia B. Margi, Katia Obraczka and J. J. Garcia-Luna-Aceves, "Modeling Energy Consumption in Single-Hop IEEE 802.11 Ad Hoc Networks", Proceeding in 13th International conference on Computer communication and networks 2004, 2004.

11. Qualnet 4.5.1 Network Security model library.pdf

12. K. Sanzgiri, D. Laflamme, B. Dahill, B. Levine, C. Shields and E. Royer. An Authenticated Routing for Secure Ad Hoc Networks. Journal on Selected Areas in Communications special issue on Wireless Ad hoc Networks, March 2005.

13. Man,Y.R.: Internet Security cryptographic: principles, algorithms and protocols. Wiley Publishing House, Chichester(2004).

14. Kimaya, S., et al.: Authenticated routing for ad hoc networks. Journal on Selected Areas in Communications 23(3), 598–610 (2005).

15. Zapata, M.G., Asokan, and N.: Securing Ad hoc Routing Protocols. In: Proc. of the ACM workshop on Wireless security, Atlanta, USA, pp. 1–10 (2002).

16. Kushwah, Virendra Singh and Tapaswi, Shashikala, "Securing Node In MANETs Using Node Based Key Management Scheme", In proceeding of the IEEE Xplore 2010 International Conference on Advances in Computer Engineering – ACE 2010, June 21-22, 2010 at Bangalore, INDIA.

17. C. Yang. Designing secure e-commerce with role-based access control. International Journal of Web Engineering and Technology, 3(1):73–95, 2007.

18. David F. Ferraiolo, John F. Barkley, and D. Ri hard Kuhn. A role based access control model and reference implementation within a corporate intranet. In ACM Transactions on Information Systems.

19. Xin Wang, Yanchun Zhang, Hao Shi ;" Access Control for Human Tasks in Service Oriented Architecture "; in IEEE/ the Fourth International Conference on Computer and Information Technology (CIT'04);2004 IEEE Computer, 29(2):38–47, 1996.

20. Mathias Kohler and Andreas Schaad . ProActive Access Control for Business Process-driven Environments. In IEEE/ Annual Computer Security Applications Conference 156 .2008.

21. Barkley, J., Beznosov, K., and Uppal, J., "Supporting Relationship in Access Control Using Role Based Access Control", Proceedings of ACM Role-Based Access Control Workshop, Fairfax, Virginia, USA, pp. 55-65, 1999.

22. Bernardi, P., Gandino, F., Lamberti, F., Montrucchio, B., Rebaudengo, M., and Sanchez, E.R., "An Anti-Counterfeit Mechanism for the Application Layer in Low-Cost RFID Devices", In International Conference on Circuits and Systems for Communications, IEEE, July, pp.207-211, 2006.

23. Xu Feng ,Lin Guoyuan , Huang Hao , Xie Li;"Role-based Access Control System for Web Services"; In Proceedings of the 4th IEEE International Conference on Computer and Information Technology ,2004.

24. Ateniese, G., Camenisch, J., and Madeiros, B. de, "Untraceable RFID tags via insubvertible encryption", Proceedings of the 12 ACM conference on Computer and communications security, November, pp.92-101, 2005.