Journal of Computer Science 9 (10): 1274-1282, 2013
ISSN: 1549-3636

doi:10.3844/jcssp.2013.1274.1282 Published Online 9 (10) 2013 (http://www.thescipub.com/jcs.toc)

MESSAGE AUTHENTICATION CODE BASED SECURE GROUP KEY MANAGEMENT PROTOCOL FOR MOBILE AD HOC NETWORKS

[1]T. Peer Meera Labbai and [2]V. Rajamani

[1]Department of Computer Science and Engineering,
SRM University, Kattankulathur, Chennai, Tami Nadu, India
[2]Department of Electronics and Communication Engineering,
Indra Ganesan College of Engineering, Manikandam, Tiruchirappalli, Tamilnadu, India

Received 2013-02-21, Revised 2013-06-27; Accepted 2013-08-22

ABSTRACT

A mobile ad hoc network is a group of nodes which are communicating with each other with the use of radio frequencies. When there is high movement of mobile nodes, the nodes find difficult to reach other nodes. If the data are exchanged between nodes when there is high mobility, the data may be lost in transit. Therefore the security of data is needed for the transmission of data. Since the high dense of mobile nodes we cannot give better security, the mobile nodes must be formed as groups. For providing security, there are pre-requirements like key establishment, key agreement and key management and so on. Then these keys are used in the encryption/decryption algorithms such as symmetric key algorithms and asymmetric key algorithms. For this study, we have taken VBOR as the base protocol. VBOR consists of two phases namely, Route discovery and Route maintenance with the use of variable bit rate. In this study, the message authentication code is generated during route discovery phase then these data are exchanged between the nodes. In this proposed work, the performance analysis is done using some performance parameters like energy consumption, packet delivery ratio, overhead and delay.

Keywords: Message Authentication Code, VBOR, Key Management Protocol, Mobile Ad Hoc Networks

1. INTRODUCTION

Wireless networks are growing rapidly in last few years. In wireless networks, there are two classifications: Infrastructure based wireless networks and Infrastructure less or ad-hoc wireless networks. Most wireless networks deployed today's life are IEEE 802.11 Wireless LANs. So there are pre established wired infrastructure for wireless LANs to connect various access points. But there are no wired connections in wireless ad hoc networks. Since the nodes are mobile nodes and there are no such pre-existing infrastructure. Nodes with wireless capability form an ad-hoc network in real time. In ad hoc network, the mobile nodes are working as a normal mobile node and as well as central coordinators which are forwarding the packets from one mobile node and another mobile node. Ad-hoc network is ideal for battlefield or rescuer areas where fixed infrastructure is very hard to deploy.

Wireless ad hoc networks, as a new wirless paradigm of wireless communication, have attracted a lot of attentions recently. An ad hoc network is considered as a collection of wireless mobile nodes that are capable of communicating with each other without the use of any centralized administration. It is formed on-the-fly and employs multi-hop routing to transmit information. The primary advantage of such a network is the underlying self-organizing and infrastructure-less property, which provides an extremely flexible method for establishing communications in situations where geographical or terrestrial constraints demand totally distributed networks, such as battlefields, emergency and disaster

Corresponding Author: T. Peer Meera Labbai, Department of Computer Science and Engineering, SRM University, Kattankulathur, Chennai, Tamilnadu, India

areas. While the great flexibility of wireless ad hoc networks also brings a lot of research challenges, one of the important issues is security. Recent researches have shown that wireless ad hoc networks are highly vulnerable to various security threats due to their inherent characteristics. As ad hoc networking somewhat varies from the traditional approaches, the security aspects that are valid in the networks of the past are not fully applicable in ad hoc networks.

A mobile ad-hoc network is a collection of autonomous nodes that communicate with each other. Ad-hoc network needs of security mechanisms for secure communication. Providing security for ad-hoc mobile nodes is a very difficult task because of they all are mobile nodes without any infrastructure. Since there is high mobility (Labbai and Rajamani, 2012) among mobile nodes we can't implement any security mechanism without a central node which is having capability to store the key pairs (Rafaeli and Hutchison, 2003; Zheng *et al*., 2006) of all mobile nodes. Suppose and the central node is moving frequently, then all key pairs of mobile nodes will be destroyed. Mobile nodes form an ad-hoc group for secure communication. In traditional wireless networks, a key distributed system is available as a third party that acts as a intermediate node between nodes of the network. Ad-hoc networks are not generally having a trusted third party. In group key agreement (Sherman and Mcgrew, 1998; Steine *et al*., 1996), multiple nodes form a group and generate a common secret key to be used to exchange information securely. A group member can leave or a new group member can join in the existing group. At that time, the group key agreement protocol needs to address the security issues related to the membership changes due to node mobility. In group key agreement protocol, all nodes within the group selects a group key for secure transmission. The membership change requires frequent change of group key. So with this algorithm, we have formed the secure algorithm with grouping the members as well as encryption.

Low resource availability necessitates efficient resource utilization and prevents the use of complex authentication and encryption algorithms. Most often, mobile nodes in ad hoc networks rely on batteries as their power source and may also have constrained computational abilities. Traditional PKI-based authentication and encryption mechanisms are relatively expensive in terms of generating and verifying digital signatures, which limit their practical application to wireless ad hoc networks. Symmetric cryptography is more efficient due to its less computational complexity, in which the communicating parties share a secret key (Rodeh *et al*., 2000; Sun *et al*., 2004). But when using it in wireless ad hoc networks, the problem is how to distribute the shared keys in the first place. It is thus challenging to develop or define some new efficient cryptographic algorithms for designing an efficient key management scheme.

In this study, a new group key management scheme and implementation of message authentication code is implemented. Compared with the PKI-based network authentication approaches, which rely on a trusted third-party server, our approach takes a self-organized way to provide the key generation and key distribution service without assuming any trust association between nodes or the existence of any centralized trusted entity in the network. Moreover, the proposed key management mechanism provides end-to-end security with less communication overhead and resource consumption.

1.1. Related Work

Papadimitratos and Haas (2002) proposed Secure Routing Protocol (SRP) based on DSR. The protocol assumes the existence of a security association between the source and destination to validate the integrity of a discovered route. In all these protocols, intermediate nodes that handle the route control messages can easily find the identity of the communicating nodes, which must be protected in case of anonymous communication.

Sanzgiri *et al*. (2002) proposed the Authenticated Routing for Ad hoc Networks (ARAN) protocol that uses public key cryptography instead of the shared security association used in the SRP. Each intermediate node running the protocol verifies the integrity of the received message before forwarding it to its neighbor nodes. Source and destination nodes use certificates included in the route discovery and reply messages to authenticate each other. The protocol has an optional second discovery stage that provides non-repudiating route discovery.

Venkatraman and Agrawal (2003) proposed an approach for enhancing the security of AODV protocol, which is based on public key cryptography. In their approach, two systems, External Attack Prevention System (EAPS) and Internal Attack Detection and Correction System (IADCS) were introduced. EAPS works under the assumption of having mutual trust among network nodes while IADC runs by having the mutual suspicion between network nodes. Every route request message carries its own digest encrypted with the sender's private key hash result in order to ensure its integrity. To validate established routes, route replies are authenticated between two neighbors along them. This approach prevents external attacks. IADC system

classifies internal attacks and sets a misbehavior threshold for each class of attack in order to detect compromised network nodes.

Zhou *et al*. (2011) proposed a hybrid key establishment scheme adopts the Logical Key Hierarchy (LKH) protocol (Steine *et al*., 1996) and Tree-based Group Diffie-Hellman (TGDH) protocol in cell groups and control group, respectively. Since LKH and TGDH are well-known key establishment schemes. However, they do not restrict key establishment protocol in each group to only LKH or TGDH. The group controller can choose an appropriate group key establishment protocol that he wants for his group according to his communication and computation environment without regard to what group key establishment schemes are being used in other groups.

SPM (Rasmussen and Capkun, 2008) is a modified link-state protocol that requires nodes joining, or leaving, the MANET to report such events to "super" nodes. Super nodes collect and distribute topology information and also handle communication between different "local" MANETs. SPM assumes that nodes periodically change their pseudonyms and that they communicate based on temporary current pseudonyms. SPM is identity-based and requires nodes to be able to retrieve each other's public keys.

2. MATERIALS AND METHODS

2.1. Proposed Scheme: Secure VBOR

2.1.1. Motivation

In mobile ad-hoc networks, the security is main concern in achieving the efficient and deployable network for military and rescuer areas. In security, there are three mechanisms to be maintained: Confidentiality, Authentication and Non-repudiation.

Confidentiality maintains that the particular message is to be received by the authorized receiver. Authentication assures that the particular message is being sent by an authorized sender. Non-Repudiation assures that any sender or receiver could not able to deny the previous transactions (Sender cannot deny that the previous message had not been sent by me or receiver cannot deny that the previous message had been received by me). If any security algorithm provides these three security mechanisms, it will be a good and deployable security algorithm. But providing these mechanisms in ad-hoc networks is difficult since there are no such infrastructures. All these mechanisms need a central authority to store the key pairs of the mobile nodes. For example, in military environment any one mobile node can be selected as a central node to which all other mobile nodes send their key pairs. In these networks, the nodes other than central node have limited power and low stability.

In this study, we have taken MAC as the security constraint. This security procedure includes the previous work of variable bit rate on-demand routing protocol (VBOR). In VBOR, the MAC algorithm is implemented to provide more security. This study has following modules:

- Grouping and Gateway member selection
- Secure key generation for VBOR
- Secure data transmission

2.2. System Model

2.2.1. Grouping and Gateway Member Selection

In mobile ad hoc network, the communication would not be possible without the proper coverage among the nodes. Because the mobile nodes are changing their location very frequently, the communication would not be possible for longer time. So the large number of mobile nodes is segmented as small groups to avoid communication breakage. By grouping the mobile nodes, we can easily identify the frequent movement of mobile nodes. Therefore the communication is taken place very efficiently without any interruption. After grouping the nodes into different groups, we have to select the gateway member node which can act as a authority for key management. The selection of gateway member is taken place by using the residual energy of the nodes which is given in VBOR. Then the gateway member is selected as per the following procedure.

2.3. Key Generation for Secure VBOR

The absence of a centralized control in wireless ad hoc networks makes key management difficult. Unlike traditional networks using dedicated nodes to support network functions, in wireless ad hoc networks all the network functions are performed by the mobile nodes themselves within the network and each one has equal functionality. For instance, packet forwarding and routing are carried out by all the mobile nodes. Due to limitations on wireless transmission range, they rely on each other in forwarding packets and each mobile node acts not only as a host, but also as a router. In such a network, there are no dedicated service nodes which can work as a trusted authority to generate and distribute the network keys. The traditional Public Key Infrastructure (PKI)-supported approach works well in wired networks, but it is inadequate for the wireless ad hoc environment. In general, PKI-based approaches require a global trusted Certificate Authority (CA) to provide certificates for the

nodes of the network and the certificates can be verified using the CA's public key. However, ad hoc networks do not possess such an infrastructure characteristics. Even if the service node can be defined, maintaining such a centralized server and keeping its availability to all the nodes in such a dynamic network is not feasible. Moreover, the service node is prone to single point of failure, i.e., by only damaging the service node, the whole network would be paralyzed. Therefore, traditional key management schemes cannot be applied directly and a distributed key management approach is needed in securing ad hoc networks.

2.4. Secure Data Transmission

In VBOR, there are two phases namely, route discovery and route maintenance. After the groups are formed and keys are generated in VBOR protocol, the route discovery is made for secure data transmission.

The route discovery phase allows a source node S that wants to communicate securely and privately with node D to discover and establish a routing path through a number of intermediate wireless mobile nodes. At first time, there are no intermediate nodes those are knowing about the source node S and destination D. The source node S triggers the route discovery phase by sending a route request message to all nodes within the group.

Secure VBOR safeguards the route discovery and makes use of some cryptographic tools. In secure VBOR, only the end nodes have to be secured. It does not impose any cryptographic validation and verification of traffic at intermediate nodes for decentralized environment, Secure VBOR poses the overhead on the end nodes, not at intermediate nodes. So the destination node acquires correct network connectivity information of various paths and the ability to choose an optimal route based on the stability of the nodes that is defined in VBOR. Finally, it produces the routing and control traffic overhead and protects end nodes against attacks. In this secure route discovery, any malicious node between source S and destination D cannot identify the original request because the MAC value is not known (since MAC is found using the shared secret key within the group) to attackers.

Our proposed work safeguards the data forwarding operation. Previous works have determined a set of diverse paths connecting the source and destination nodes. It introduces limited transmission redundancy across the paths, by dispersing a message into N fragments. So the successful reception of any range of fragments allows the reconstruction of the original message at the destination. Each fragment equipped with a cryptographic header that provides integrity and secure exchange along with origin authentication and is transmitted over one of the paths. The destination generates an acknowledgement informing the source about the reception of fragments. Otherwise the source retransmits all the fragments after the negative acknowledgement. In this study, we have proposed that it sends the whole data with cryptographic parameters along with VBOR routing protocol.

Finally with help of security, the VBOR protocol will forward the data packets securely to the destination. Since the message is transmitted by encrypting it using the master and shared key of that particular group. Thus any malicious node between source and destination cannot decrypt the scrambled message since the shared key has been generated among the particular members of that group.

2.5. Operation

2.5.1. A Route Discovery

A source node 'S' maintains a Query Sequence number (Q_{SEQ}) for each destination it securely communicates with. This 32 bit sequence number increases for each route request generated by S and allows T to detect outdated route request. For each of the outgoing Route Request, S generates a 32bit random Query Identifier (Q_{ID}), which is used by intermediate nodes as a means to identify the request.

Both Q_{ID} and Q_{SEQ} are input to the Message Authentication Code (MAC) along with route request message, security association number, source address and destination address. Then the whole information is encrypted using the shared secret key $S_{i,j}$ of that group. The Message Authentication Code M is calculated as Equation 1:

$$M = C(S_{i,j}\{RREQ, SA_{num}, Q_{id}, Q_{seq}, SA, DA\}),\ SA,\ DA \qquad (1)$$

This is the message, the secure VBOR sends through intermediate nodes towards destination. This MAC value will be sent through intermediate nodes towards destination. The security of this proposed work lies in calculating MAC value. In **Fig. 1**, the intermediate nodes M1 and M2 cannot decrypt the MAC value because shared secret key of source and destination is only known to the source and destination but not to intermediate nodes. Thus it provides more security for the messages and it avoids message tampering attack. The procedure for Gateway Member Selection and key generation of proposed scheme are discussed in **Table 1 and 2** respectively.

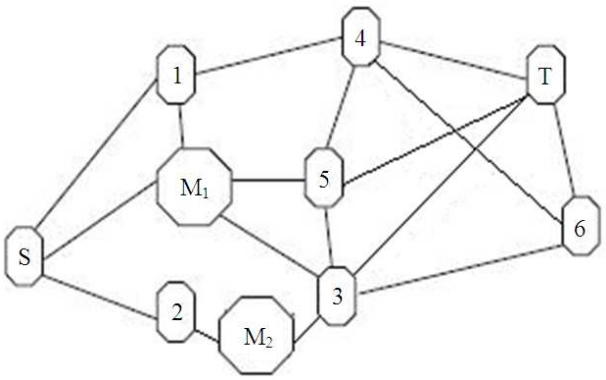

Fig. 1. Source S communicates with Destination T through malicious nodes M_1 and M_2

Table 1. Gateway member selection

Network is separated into groups
Subgroups are generated by using the total number of nodes and number of subgroups that are needed and it is restricted to 'n'.
that is, $S = N/N_S$ and $S \leq n$
Select gateway member if the residual energy of the node is greater than the
threshold residual energy
If ($E_R > R_{th}$)
then $G_m = S[M_i]$
where $S[M_i]$ is the member of the subgroup S
Find the private key and public key pair for each member $S[M_i]$
If a new node 'i' enters into the subgroup S, a new gateway member is selected.
Then follow step 3.

Table 2. Key generation

User i generates it's private key PR_i
User j generates it's private key PR_j
User i and j calculate their public key such as
$PU_i = PR_i * G$
$PU_j = PR_j * G$
where G is the generated point in public key cryptography
User i sends its public key to user j
5. User j computes group key such that
$S_j = PR_j * PU_i$
User j sends its public key to user i
User I computes group key such that
$S_i = PR_i * PU_j$
Check $S_j = S_i$
9. If they are same then the gateway member stores this key as $S_{i,j}$

Table 3. Simulation setup

Parameter	Value
Test Area	1500×1500m
Channel type	Wireless channel
Radio Propagation	Two Ray Ground
Antenna type	Omni antenna
Interface Queue type	Drop tail with priority queue
Interface Queue length	50
Transmission Range	250m
Number of Nodes	100
Transmission Bandwidth	1Mbps
MAC	IEEE 802.11
Mobility Model	Random Waypoint
Traffic type	VBR, UDP
Packet Size	512 bytes
Initial Energy	100 Joules

2.6. Simulation Parameters

NS2 [2.3.5] is used as the simulator for estimating the performance of the nodes under conventional path routing and proposed routing in presence of the malicious nodes. The simulation setup parameters are listed below in **Table 3**.

Intermediate nodes relay route request, so that one or more query packets arrive at the destination. The route requests reach the destination D, which constructs the route replies it calculates a MAC covering the route reply contents and returns the packet to S over the reverse of the route accumulated in the respective request packet. The destination responds to one or more request packets of the same query, so that it provides the source with a diverse topology picture as possible. The querying node validates the replies and updates its topology view.

3. RESULTS

3.1. Performance Analysis

Simulation study has been carried out to show the performance of the proposed secure VBOR protocol. Simulation results have been compared for different number of nodes 30, 40 and 50 in terms of energy consumption, packet delivery ratio, overhead and delay.

Average energy consumption with the speed of nodes is depicted for secure VBOR depicted in **Fig. 2**. It is the energy consumption for different number of nodes 30, 40 and 50 with speed. The figure shows that the energy consumption for 30 nodes starts at 10 joules for the speed 1 m s^{-1} but it increases when the speed of the nodes increases. Likewise, the energy consumption for 40 and 50 nodes are also increased when the speed increases.

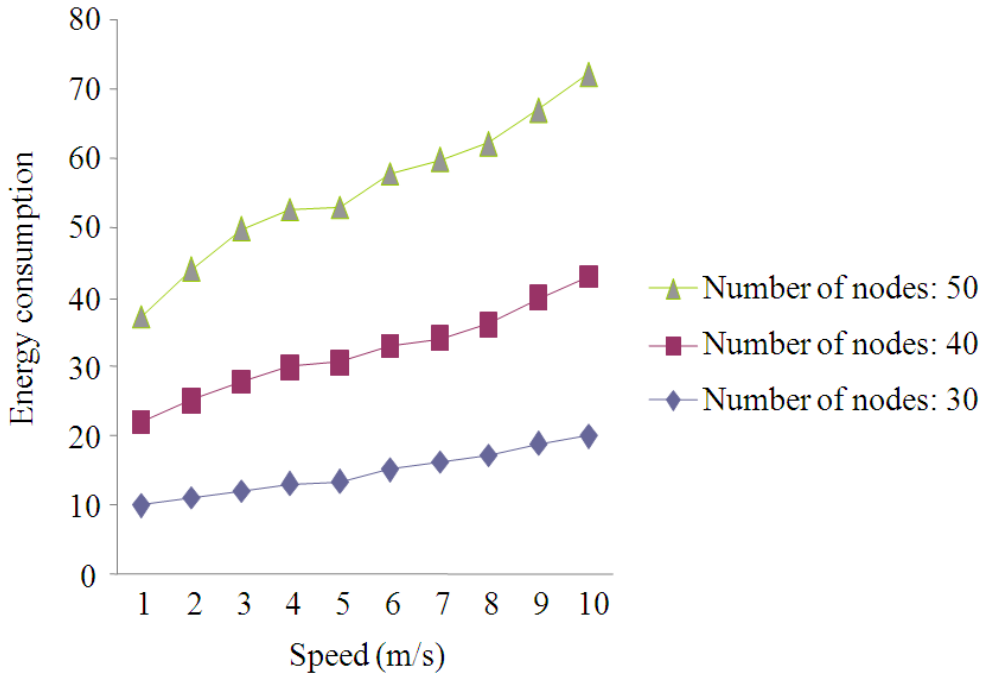

Fig. 2. Variation of energy consumption with speed

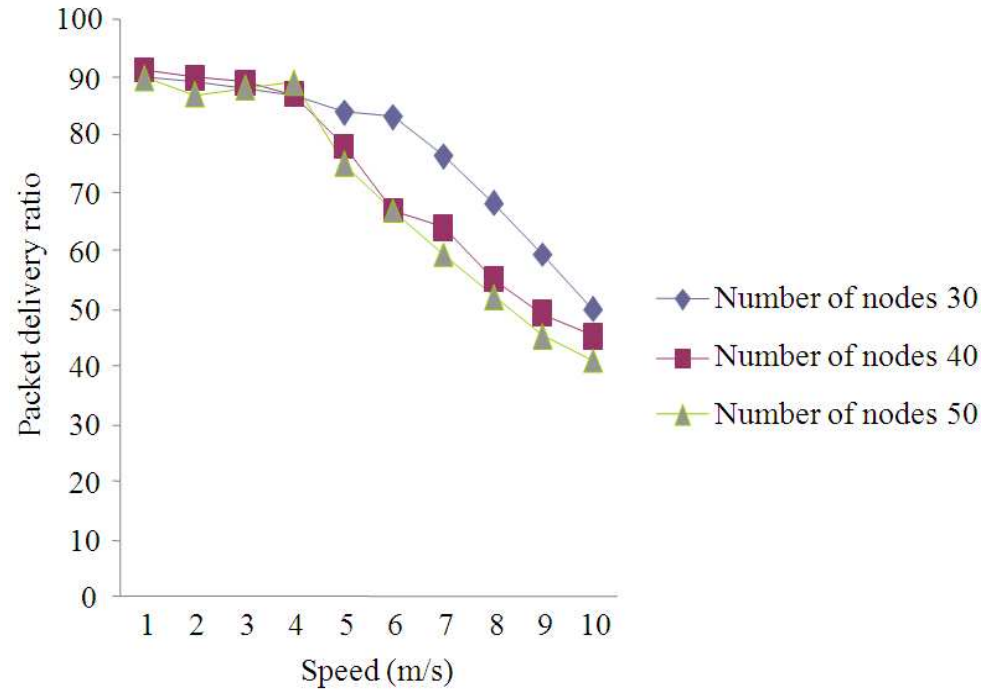

Fig. 3. Variation of packet delivery ratio with speed

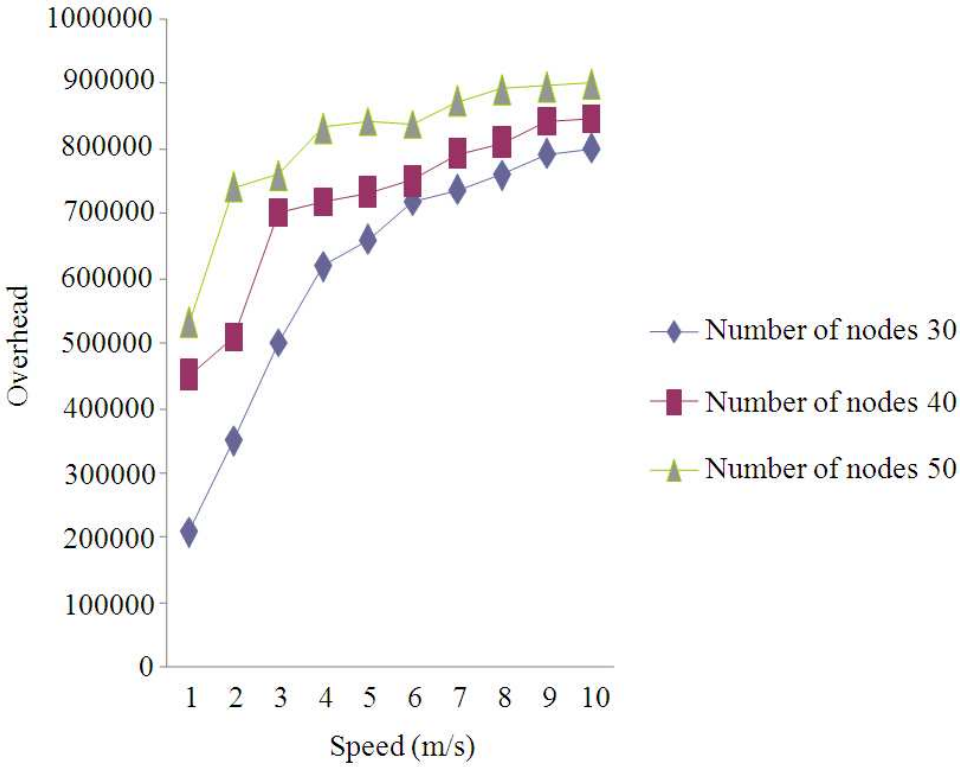

Fig. 4. Overhead with speed

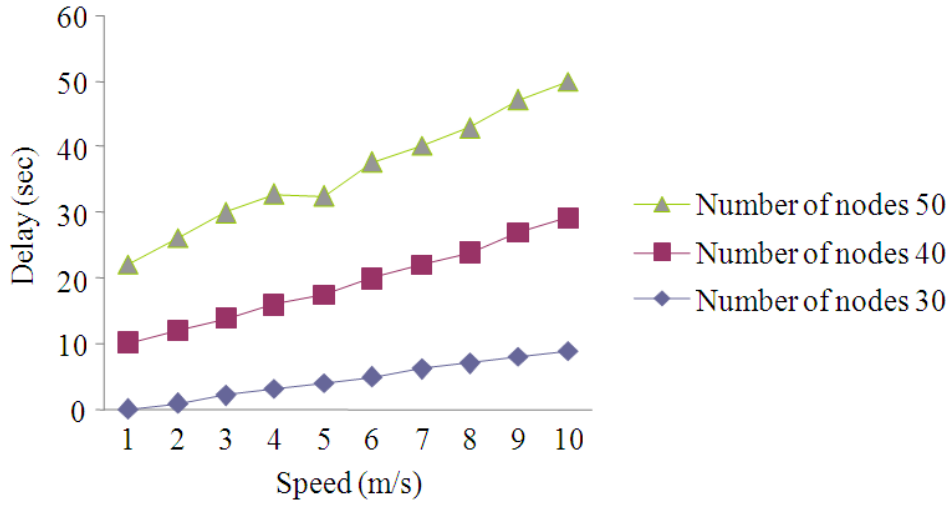

Fig. 5. Variation in delay with speed

Variation of packet delivery ratio with speed is shown in **Fig. 3**. Data delivery ratio can be calculated as the ratio between the number of data packets that are sent by the source and the number of data packets that are received by the destination. Packet delivery ratio decreases when the speed increases for all 30, 40 and 50 nodes. 90% packet delivery ratio is decreased to 40% due to maximum speed.

Figure 4 shows the variation in overhead with speed in route discovery phase. The control messages where high due to frequent path breaks during mobility and energy depletion of nodes. Here overhead should be high since the formation of groups yields too much overhead for maximum of 50 nodes since the control messages are to be transmitted continuously when speed increases.

Variation of data transmission delay with speed is depicted in **Fig. 5**. Packet transmission delay of Secure VBOR is very low for 30 nodes compared with 40 and 50 nodes at beginning and it goes to top level that is almost 90% because of the time taken to form the groups and sharing of secret keys. When the member joins/leaves, the groups should be reformed and keys are changed. Thus it takes delay in data transmission as well as in key formation.

4. DISCUSSION

In this study of our article, it is observed and determined that when there is high mobility of nodes and data exchange takes place, some data gets lost in the transit. The proposed method states that the mobile nodes must be formed as groups for better security .It generates message authentication code during route discovery phase and then data exchange takes place. It is found that the Secure VBOR protocol exhibit better performance in terms of energy consumption, packet delivery ratio, overhead and delay, when compared for a set of nodes 30, 40, 50. This protocol provides a good performance for mobile ad-hoc networks that can be effectively used.

5. CONCLUSION

MANET needs more security because of the nature of mobile nodes. This study gives security to the Variable Bit rate on demand Routing protocol (VBOR). When compared symmetric key cryptography, public key cryptography gives more security to the ad hoc networks because the nodes have to secure their keys with themselves. Here the malicious nodes cannot get the data since the message authentication code is computed within the group members. Thus the MAC value should be known to the group members. In this study, the nodes are authenticated and then the group members are decided also the gateway member is selected based on the residual energy of the nodes. The data is transmitted with confidentiality that is no malicious and selfish node cannot get the MAC value.

6. REFERENCES

Labbai, T.P.M. and V. Rajamani, 2012. A variable bit-rate on-demand routing protocol for mobile ad hoc networks. Int. J. Ad Hoc Sensor Ubiquit. Comput., 3: 31-40.

Papadimitratos, P. and Z.J. Haas, 2002. Secure routing for mobile ad hoc networks. Proceedings of the SCS Commnication Networks and Distributed Systems Modeling and Simulation Conference, Jan. 27-31, San Antonio, TX., pp: 194-204.

Rafaeli, S. and D. Hutchison, 2003. A survey of key management for secure group communication. ACM Comput. Surveys, 35: 309-328. DOI: 10.1145/937503.937506

Rasmussen, K.B. and S. Capkun, 2008. Location privacy of distance bounding protocols. Proceedings of the 15th ACM Conference on Computer and Communications Security, Oct. 27-31, ACM Press, New York, USA., pp: 149-160. DOI: 10.1145/1455770.1455791

Rodeh, O., K.P. Birman and D. Dolev, 2000. Optimized group rekey for group communication systems. Proceedings of ISOC Network and Distributed Systems Security Symposium, (SSS' 00). CiteSeerX.

Sanzgiri, K., B. Dahill, B.N. Levine, C. Shields and E.M. Belding-Royer, 2002. A secure routing protocol for ad hoc networks. Proceedings of the 10th IEEE International Conference on Network Protocols, Nov. 12-15, IEEE Xplore Press, pp: 78-87. DOI: 10.1109/ICNP.2002.1181388

Sherman, A.T. and D.A. Mcgrew, 1998. Key establishment in large dynamic groups using one-way function trees. IEEE Trans. Soft. Eng., 29: 444-458. DOI: 10.1109/TSE.2003.1199073

Steine, M., G. Tsudik and M. Waidner, 1996. Diffie-hellman key distribution extended to group communication. Proceedings of the 3rd ACM Conference on Computer and Communications Security, Mar. 14-15, ACM Press, New York, USA., pp: 31-37. DOI:10.1145/238168.238182

Sun, Y., W. Trappe and K.J.R. Liu, 2004. A scalable multicast key management scheme for heterogeneous wireless networks. IEEE/ACM Trans. Network., 12: 653-666. DOI: 10.1109/TNET.2004.833129

Venkatraman, L. and D.P. Agrawal, 2003. Strategies for enhancing routing security in protocols for mobile ad hoc networks. J. Parallel Distrib. Comput., 63: 214-227. DOI: 10.1016/S0743-7315(02)00065-5

Zheng, M., G. Cui, M. Yang and J. Li, 2006. Scalable group key management protocol based on key material transmitting tree. Proceedings of the 3rd International Conference on Information Security Practice and Experience, May 7-9, Springer Berlin, Heidelberg, Hong Kong, China, pp: 301-313. DOI: 10.1007/978-3-540-72163-5_23

Zhou, H., M. Zheng and T. Wang, 2011. A novel group key establishment scheme for MANETs. Proc. Eng., 15: 3388-3395. DOI: 10.1016/j.proeng.2011.08.635