ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2019.0283

IMPLEMENTATION OF A CRYPTOGRAPHY TECHNIQUE TO PREVENT WORMHOLE ATTACK

K. Sundaravadivel

Department of Computer Science, Thiru Govindasamy Government Arts College, India

Abstract

Mobile Ad-hoc network (MANET) is a decentralized type of wireless network. Due to its low cost of installation and easy maintenance, it is always self-configuring, infrastructure-less network of mobile devices associated with wirelessly. Every device in a MANET is free to move separately in any direction, and will therefore change its associations with the other devices regularly. Mobile ad-hoc network is similar kind of network where the device working as both sender and receiver. In this network, the device to device communication is usually has a routable networking environment on top of a Link Layer. Therefore, an intermediate host always becomes a part of communication. If the intermediate host is not trusted, then it can be modifying the messages transmitted to towards the destination host. A mechanism is necessary to improve the present communication technique in mobile ad-hoc network. So, we have used the cryptography technique. Then, the security in ad-hoc networks is investigate. The investigation leads to find a solution for wormhole attack. In this attacker, a group of attacker is deployed in the network and troubles the privacy and security of the network. Therefore, a solution with the cryptographic technique to prevent the information forward to the destination is proposed. The second contribution of the work is to prepare a technique by which the wormhole nodes are prevented in the network. The implementation of the proposed work is performed on the NS2 network simulator and the generated trace files are used for performance evaluation of the work. The performance of the proposed routing protocol evaluates the in conditions of end to end delay, throughput, packet delivery ratio, and packet drop ratio and also validate the solution for the proposed routing protocols performance is compared with the established EAACK and the AODV routing protocol. According to the experimental results, the performance of the proposed routing protocol is found optimum and adaptable for both security and performance issues in the network.

Keywords:

Cryptography, Wormhole Attack, Routing protocol, AODV, EAACK, Mobile Ad-hoc Network

1. INTRODUCTION

Mobile Adhoc network is a kind of wireless network. Wireless networks have become the most common areas of research in the networking. Ad hoc network allows the devices to maintain links to the network as well as easy to add and remove devices to and from the network. The set of applications for MANET are various ranging from large-scale mobile highly dynamic networks, to small, static networks that are controlled by power sources. Besides the legacy applications that move from traditional infrastructure environment into the ad hoc context, a great deal of new services can and will be generated for the new environment [1]. It includes the Military Battlefield, Sensor Networks, Medical Service and Personal Area Network. MANET almost used in army application, disaster relief teams and monitoring.

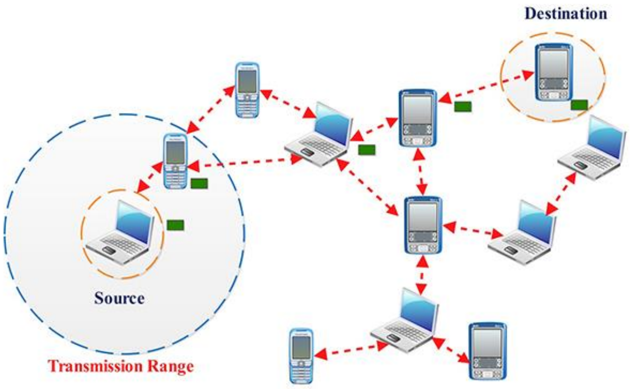

Fig.1. Mobile Ad-Hoc Network

1.1 DOMAIN OVERVIEW

A Mobile Ad Hoc Network (MANET) [1]–[10] is an interrelated system of wireless nodes which is communicate with the over bandwidth controlled wireless links. Every wireless node can function as a sender, a receiver or a router. After the node is a sender, it can send messages to any particular destination node through some route. Because a receiver, it can receive messages from other nodes. While the node functions as a router, it can communicate the packet to the destination or after that router in the route. When necessary, each node can buffer packets awaiting transmission [2].

1.1.1 Overview of the Mobile Ad-hoc Network System:

The mobile ad hoc network is a kind of wireless network. Due to this, the nodes are lashed with the Wi-Fi ability, but due to Wi-Fi the nodes have a limited range for communication therefore to communicate long distance nodes the relay options are used. Additionally, to establish a connection between communicating routing protocols are responsible. The routing protocols are used for discovering shortest path and maintain the routes during the path break. Additionally, the network supports the mobility due to this any node can leave or join the network anytime. Thus, most of the attackers are tries to deploy attacks through the routing protocols [3] [14] – [23]. In this work, the wormhole attacks are considered and investigated solution development.

1.1.2 Overview of Wormhole Attack:

The wormhole is a kind of internal attack with more than one attacker is involved for deployment of attack. The attackers are using high-speed connections among the attackers involved. This high-speed link is known as wormhole link due to the speed this link attracted a significant amount of traffic and when packets are queued in this link the jam situation is occurring. This kind of network fault is known as the wormhole attack. The complexity of this attack is increased attackers are also in mobile mode [6].

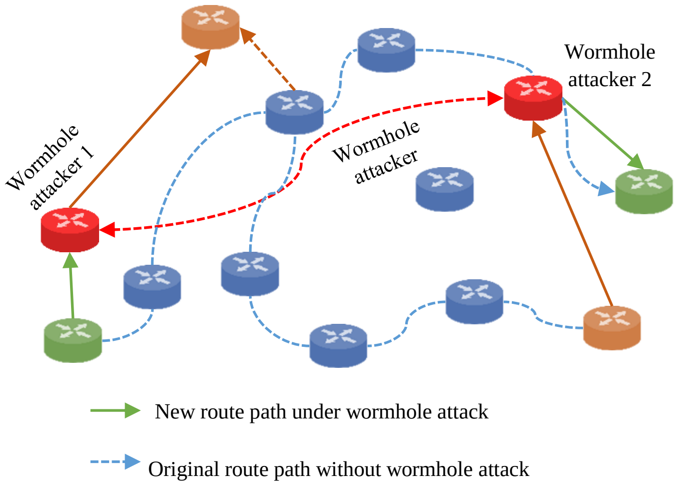
Wormhole attacker 1
Wormhole attacker
Wormhole attacker 2
New route path under wormhole attack
Original route path without wormhole attack

Fig.2. Wormhole attack

1.1.3 *Enhanced Adaptive Acknowledgement (EAACK):*

EAACK Intrusion detection system is an IDS which is used to detect all the attacks that take place in the node which acts as route for packet transmission from source to destination in AODV protocol. It is activated in Network layer of the protocol stack.

Each node contains its own secret private key and public key and each message is digitally signed for authentic purpose. The proposed scheme identifies when the node becomes malicious due to interaction by other nodes in the network. It identifies the selfish node due energy loss that cannot involve in further packet transmission. When a malicious node is identified packet transmission is stopped and new route discover process is handled by the AODV protocol and transmission of packets are preceded [11] [12]. The EAACK mechanism is initiated after the route is discovered from source to destination.

EAACK is consisted of three major parts. Namely,

- Acknowledge (ACK)
- Secure-Acknowledge (S-ACK)
- Misbehavior Report Authentication (MRA)

1.1.4 *Overview of AODV Routing Protocol:*

AODV routing protocol is basically a combination of DSDV and Data Source Routing (DSR) protocols. It borrows the essential on-demand mechanism of route discovery and route maintenance from DSR, advantage the use of hop-by-hop routing, sequence numbers, and periodic beacons from DSDV. AODV routing algorithm minimizes the number of required broadcasts by creating routes only on-demand basis and enables dynamic, self-starting and multi-hop routing between participating mobile nodes by wishing to establish and maintain an ad hoc network [12]. The routing messages in AODV do not contain information about the complete route path, but only about the source and the destination. The message types defined by AODV are Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) [13] [14].

2. LITERATURE SURVEY

In [1], the authors center on basic security attacks in Mobile ad-hoc networks. MANET has no obvious line of protection, so, it is easy to get to both valid network users and malicious attackers. In the existence of malicious nodes, one of the main challenges in MANET is to design the forceful security explanation that can defend MANET from a variety of routing attacks.

In [2], the author presents an overview of MANET knowledge, its key uniqueness and how it can be leveraged for the Third Generation Singapore Armed Forces. Knowledge gain and training learnt from an experimentation begin and funded by the Future Systems Directorate on MANET are also discussed.

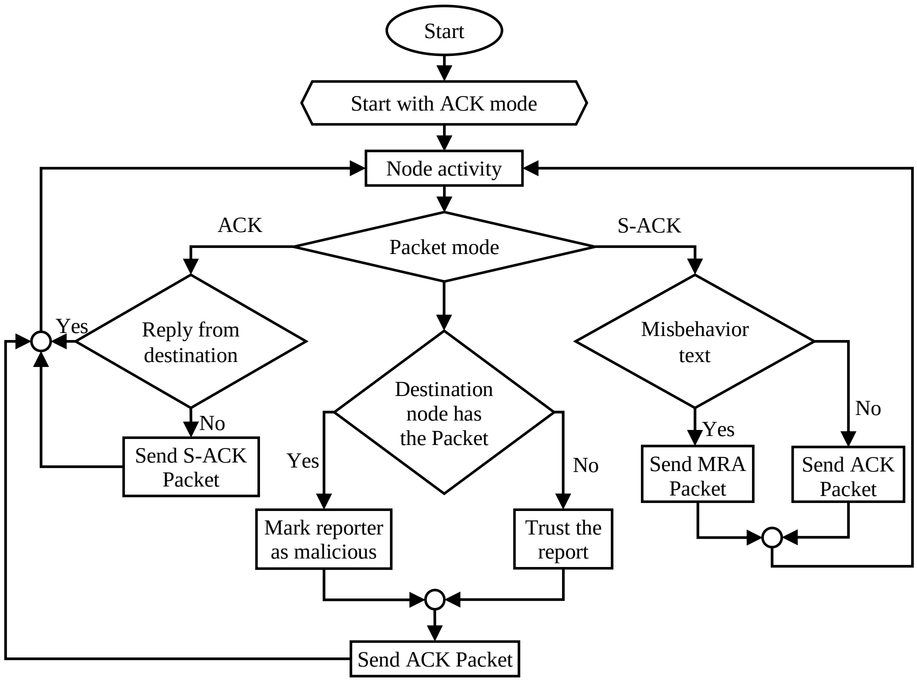

Fig.3. EAACK

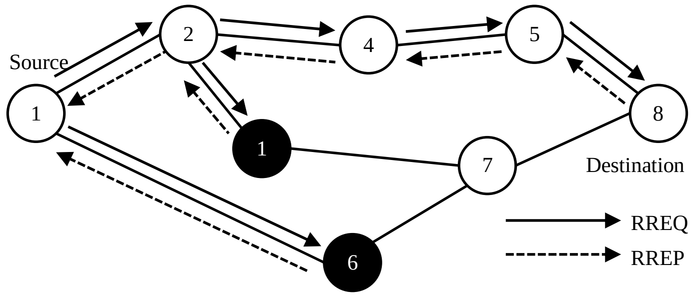

Fig.4. Adhoc Demand Distance Vector

In [3], the authors provide the summary of classification routing protocols and also provides a comparison between them. In spite of many stimulating future applications of mobile ad hoc networks (MANETs), there are still some critical challenges and open problems to be solved. Thus, broadly in this paper we present an overview of MANETs, and their routing protocols.

In [4], the authors focus on the wormhole attack, its categorization and the modes by which they are launched. This paper summarizes various detection techniques proposed for wormhole attack and also present the effect of wormhole attack on various performance parameters.

3. PROPOSED METHOD

We have used the cryptography technique. Cryptography is a related with the process of converting the ordinary plain text into unintelligible text and vice-versa. It is a method of store and transmits the data in a particular form. Cryptography method is a not only protect the data from robbery or modification, but also be used for user substantiation.

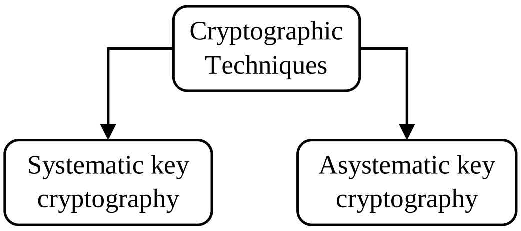

Fig.5. Cryptography Techniques

In this Cryptography technique, we are using two methods, namely, Diffie Hellman Key Exchange and RC5.

3.1 DIFFIE HELMAN KEY EXCHANGE

Diffie Hellman Key Exchange methods is a strong solution for secure key exchange over the untrusted network environment.

3.2 DIFFIE-HELLMAN KEY EXCHANGE ALGORITHM STEPS

Step 1: User *A* generate the domain parameters *p*, *q* and *g*.

Step 2: User *A* generates a random private key X_A.

Step 3: User *A* calculates public key as $Y_A = g^{X_A}$ mod *p*.

Step 4: User *A* sends (p, g, Y_A) to user *B*.

Step 5: User *B* generates a random private key $X_{B.}$

Step 6: User *B* calculates public key $Y_B = g^{X_B}$ mod *p*.

Step 7: User *B* calculates as

$$K = (Y_A)^{X_B} \bmod p = (g^{X_A})^{X_B} \bmod p = g^{X_A \cdot X_B} \bmod p$$

Step 8: User *B* sends the Y_B to user *A*.

Step 9: User *A* calculates as

$$K = (Y_B)^{X_A} \bmod p = (g^{X_B})^{X_A} \bmod p = \mathrm{g}^{X_A \cdot X_B} \bmod p.$$

3.3 RC5 (RIVEST CIPHER)

RC5 method is used to encrypt and decrypt the data.

Algorithm

```
begin
    $A$: = ($A$ <<< $S$ [0]) + $S$ [0];
    $B$: = ($B$ <<< $S$ [1]) + $S$ [1];
    for $i$ = 1 to $r$ do
        $A$: = ($A$ <<< $S$ [$i$]) + $S$ [$i$+1];
        $B$: = ($B$ <<< $S$ [$i$+1]) + $S$ [$i$+2];
            $A$: = (($A \oplus B$) <<< $B$) + $S$ [$2 * i$];
            $B$: = (($B \oplus A$) <<< $A$) + $S$ [$2 * i + 1$];
    end;
end;
```

4. EXISTING METHOD

This paper has considered and taken the EAACK approach for study purpose and comparison only.

4.1 EAACK ALGORITHM STEPS

Step 1: A secret private key and public key is generated in advance and each message is digitally signed with cryptography algorithm for authentic process.

Step 2: Sends the ACK Packet 2-b to the nodes from source to destination.

Step 3: The Destination *D* must send the Acknowledgement packet within the time line.

Step 4: If the node *D* sends the ACK packet in time, then the node is in normal mode.

Step 5: If D does not send the ACK packet in the given timeline, then the S-ACK mode will be activated.

Step 6: If S-ACK reports in time, then the node is normal.

Step 7: If S-ACK reports a false misbehavior report or if S-ACK does not report to the source *S* within the time line, MRA mode is activated.

Step 8: MRA scheme sends the 2-b packet, verifies the node with report provided by S-ACK report.

Step 9: If the node provides the same report as S-ACK then the node is reported as malicious node.

Step 10: If the node *D* does not contain the packet, then the node is reported normal.

5. IMPLEMENTATION

This chapter provides the information about implementation and simulation configuration.

5.1 NETWORK SIMULATION SETUP

In this section, the necessary network pattern of the proposed approach implementation is described. In adding to their parameter and the necessary values are too reported. The Table.1 contains the network simulation setup parameters and their reports.

Table.1. Network Simulation Setup

Simulation Properties	Values
Antenna model	Omni Antenna
Simulation area	750×550 or 1000×1000
Radio propagation Model	Two Ray Ground
Channel type	Wireless Channel
No of mobile Nodes	20,30,50,80,100
Routing Protocol	AODV

6. SIMULATION SCENARIO

In organize to do the experiments, the following experimental scenarios are established in the proposed work.

6.1.1 Simulation of the Usual Network Base EAACK:

A MANET initially configured by the help of AODV routing protocol. In this simulation, we configure the network according to base approach. We developed EAACK, which method giving a large number of packets. In this network, the wormhole link is introduced using the high link off the channel in wireless communication. In this scenario, two colluding nodes are receiving packets. The attacker drops the packet or transfer packet after modified that packet. Therefore, routing is troubled and sensitive information capture by the malicious node. In this network the green nodes are denoted the client nodes of the network, blue nodes are denoted by the sender and receivers of the network and the red nodes represent by the attacker nodes of the network.

6.1.2 Simulation for the Proposed Secure Routing Protocol:

In order to represent the efficiency of the proposed routing protocol a network with the proposed routing technique is configured and as a similar previous scenario the network attackers are introduced in the network. After that the performance of the network in similar parameters are computed and compare with the previous scenario's outcomes. In this network the green color nodes represent the normal client nodes, blue nodes represent the sender and receiver of the network and finally, the attackers or wormhole link is offered using red color nodes.

6.2 RESULTS AND DISCUSSIONS

After implementation of the proposed work concept for the mobile ad hoc network. In this chapter provides the study about the computed performance of the both scenarios. So the measured performance of the implemented techniques is validating by the different parameters.

6.2.1 End to End delay:

End to End Delay is the time in use for a packet to be transmit across a network from source to destination. That time usually computed in term of milliseconds. E2E Formula is expressed as below,

E2E = *Receiving time – Sending Time*

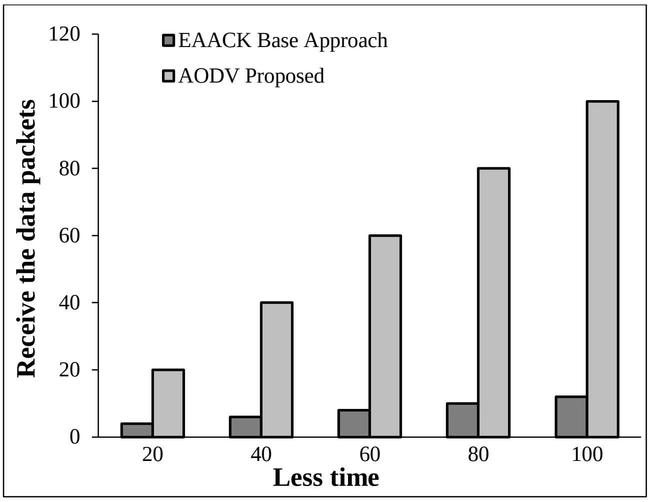

Fig.6. End to End delay

These parameters measure end to end delay of the network of under attack condition for evaluating both scenarios namely the proposed work and the traditional AODV routing is validated using Fig.8. The end to end delay parameter of the proposed work is validated the red chart graph and the green chart graph showing the performance of the base approach techniques. In this performance evaluating, the proposed techniques require less time as comparing to the base technique for delivering the data packet across the network. Because owing to attacker's affect the network is overloaded owing to this travelling time of the packet are increased as compared to usual scenarios. So, this proposed technique is adaptable as compared to EAACK routing protocol.

6.2.2 Routing Overhead:

Throughput is the number of packets successfully received at the destination per unit's time. It gives the total number of routing packets transmitting through the simulation. It is the ratio of routing packets to the total number of packets generate by the source.

Routing overhead = Number of sent routing packets / Total number of received packets

The routing overhead of both the simulated scenarios namely EAACK approach and AODV proposed secure technique are established using Fig.9. The X axis represent by the number of nodes in the network and also, the Y axis denoted by a number of packets moreover inject in the network. For representing the performance of both the scenarios the red line is used for proposed method and the blue line is used for previous routing protocol. According to obtain the experimental results, the proposed technique requirement for the less amount of manage the message exchange as compare to the previous one. Since due to the effect of attacker node some time retransmission occurs and increase the network routing overhead. Therefore, the proposed technique is capable to decrease the effect of network attackers and optimizes the performance of network under the attack condition.

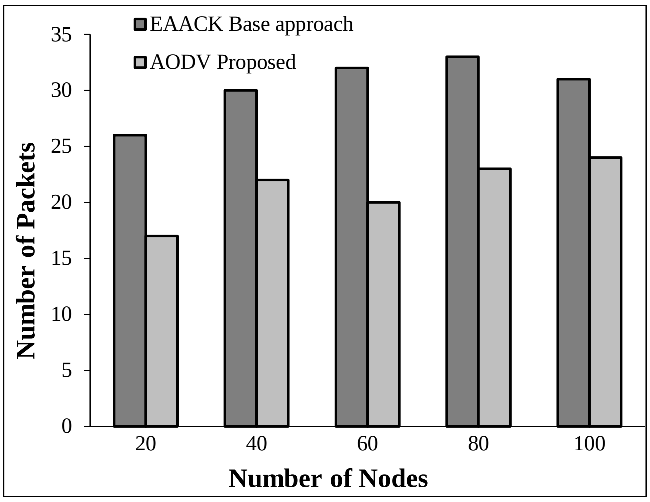

Fig.7. Routing Overhead

6.2.3 *Residual Energy:*

In wireless network for each event such as sending and receiving of packets an amount of energy required. Therefore, after performing the simulation with the network an amount of energy consumed. The balance amount of energy of the network is term the residual energy of network.

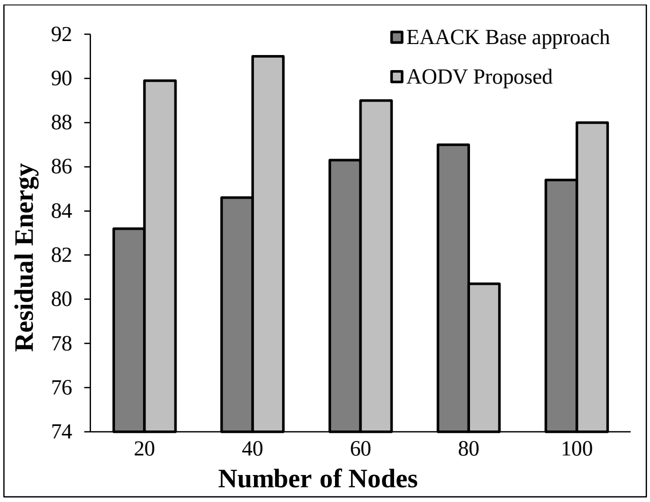

Fig.8. Residual Energy

The Fig.8 shows the remaining average energy of network for both the network scenarios. In this diagram, the X axis represents the number of nodes in the network and also, the Y axis represent the related to energy remain in the network. For the show of the proposed technique, the red line graphs are used similarly the blue lines are used for representing the performance of EAACK base approach for under the attack conditions. According to the obtain performances, the proposed method requires the less amount of energy for communication as compared to the previous routing algorithm in the similar network configuration and attack conditions. Thus the proposed technique preserves the network from the attacker's effect more successfully.

6.2.4 *Packet Delivery Ratio:*

The Packet delivery ratio is also called the PDR ratio. The packet delivery ratio provides the information about the performance of any routing protocols using the successfully delivered packets to the destination.

PDR = Total Delivered Packets/Total Sent Packet

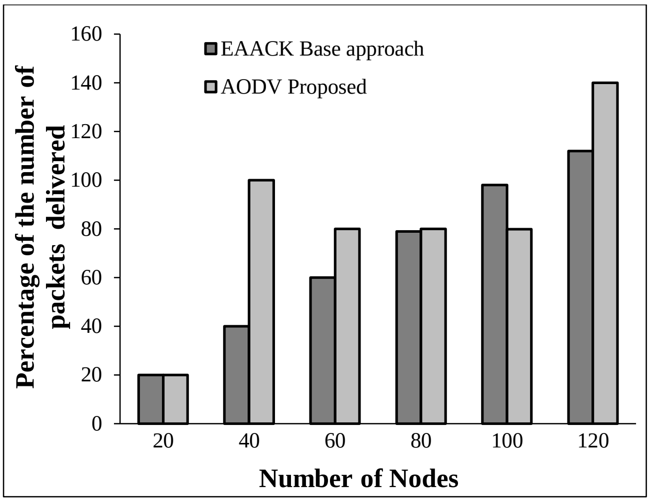

Fig.9. Packet Delivery Ratio (PDR)

The packet delivery ratio under the wormhole attack conditions is evaluated for both the network scenarios using the Fig.9. This figure, the X axis denoted by the number of nodes in the network during the simulation and also, the Y axis denoted by the percentage number of packets successfully delivered. The red lines in the given graph show the performance of proposed technique and the blue line graphs are simulating the EAACK routing protocol. According to the experimental outcome, the proposed technique is capable to successfully neglect the outcome of attackers. Due to this the network performances maintain for as required but in normal network conditions, the considerable amount of packet loss is observed. Thus the proposed system is flexible for preventing the wormhole attack in the network.

6.2.5 *Throughput:*

Network throughput is the common rate of successful delivery of a message more than a communication medium. This data may be transmitted over a physical or logical link, or pass through a certain network node. The throughput is intended in terms of bit's or bps, and infrequently in terms of data packets per time slot or data packets per seconds.

Throughput = Number of packets sent/Time taken

The throughput of both the routing techniques is given using Fig.10. The measurement of throughput is given here in terms of a kilobyte per seconds. For representation of performance graphically X axis denotes the number of nodes in the network during simulation and the Y axis demonstrates the consumed bandwidth of the network. The red line in this graph shows the throughput of network using proposed approach and the blue line show the performance of EACCK base approach. Experiments with the different number of nodes shows the performance of proposed technique is not affected even when the attacker exists on the network. Therefore, the technique is able to neutralize the effect of attackers in the network thus the proposed approach is suitable for use with the MANET routing.

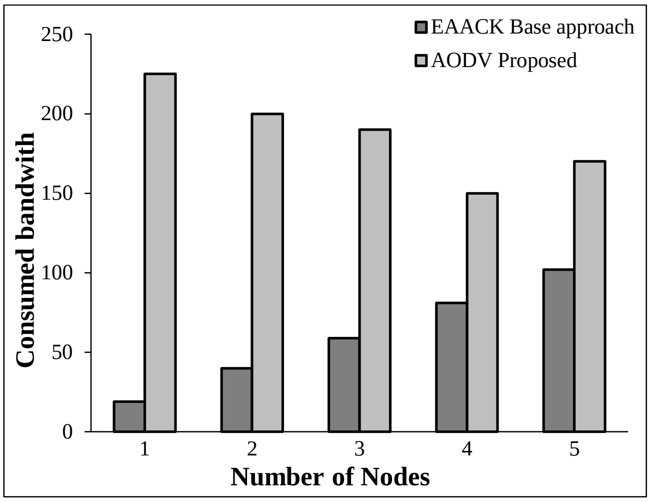

Fig.10. Throughput

7. FINDINGS

The implementation of the proposed method is performed using the NS-2 network simulator. Additionally, to implement the required concept the AODV routing is used. After implementation of desired routing technique, the evaluation process compared to proposed technique performed under attack conditions. For comparison validate the both different parameters with increasing the network size which is validated and reported.

Table.2. Compared to different parameters

Parameters	Proposed techniques	Base EAACK techniques
End to End Delay	Low	High
Packet Delivery Ratio	High	Low
Throughput	High	Low
Remain Energy	High	Low
Routing Overhead	Low	High

8. CONCLUSION

The main aim of the proposed work is to improve the performance and security of the mobile ad hoc network. Therefore, the traditional routing protocol with the new concept is modified for preventing the wormhole attack. The mobile ad hoc network is vulnerable to various kinds of attacks, among most of the attacks are deployed on the basis of poor routing protocol design. Therefore, it is required to improve the security during routing of data packets. So a cryptographic technique is proposed to secure the routed data and prevention of attacker. In order to encrypt and decrypt the data RC5 encryption algorithm is used and for secure key exchange between both the communicating parties the Diffie-Hellman key exchange process is used, which ensures the data is only decrypted by the node which has the valid key for communication.

REFERENCES

[1] Priyanka Goyal, Sahil Batra and Ajit Singh, “A Literature Review of Security Attack in Mobile Ad-Hoc Networks”, *International Journal of Computer Applications*, Vol. 9, No. 12, pp. 11-15, 2010.

[2] Elhadi M. Shakshuki, Nan Kang and Tarek R. Sheltami, “EAACK-A Secure Intrusion-Detection System for MANETs”, *IEEE Transactions on Industrial Electronics*, Vol. 60, No. 3, pp. 1089-1098, 2013.

[3] M. Kashap, S. Sing and R. Kumari, “Routing Issues and Challenges for MANET: A Review”, *International Journal of Engineering Research and Technology*, Vol. 2, No. 10, pp. 23-34, 2013.

[4] F. Wu, “Economic Incentive Mechanisms for Wireless Ad Hoc Networks Principal Investigator”, *Natural Science Foundation of China*, Vol. 12, No. 3, pp. 23-35, 2012.

[5] A. Valarmozhi, M. Subala and V. Muthu, “Survey of Wireless Mesh Network”, *International Journal of Engineering and Innovative Technology*, Vol. 2, No. 6, pp. 338-242, 2012.

[6] Guoyou He, “Destination-Sequenced Distance Vector (DSDV) Protocol”, Technical Report, Networking Laboratory, Helsinki University of Technology, pp. 1-9, 2002.

[7] Ravinder Ahuja, Alisha Banga Ahuja and Pawan Ahuja, “Performance Evaluation and Comparison of AODV and DSR Routing Protocols in MANETs under Wormhole Attack”, *Proceedings of 2nd IEEE International Conference on Image Information Processing*, pp. 699-702, 2013.

[8] Nikhil Kumar, Vishant Kumar and Niti Kumar, “Comparative Study of Reactive Routing Protocols AODV and DSR for Mobile Ad hoc Networks”, *International Journal of Computer Science and Information Technologies*, Vol. 5, No. 5, pp. 6888-6891, 2014.

[9] Charles E. Perkins and Elizabeth M. Royer, “Ad-Hoc On-Demand Distance Vector Routing”, Technical Report, Sun Micro Systems Laboratories, Advanced Development Group, 1996.

[10] P. Ning and K. Sun, “How to Misuse AODV: A Case Study of Insider Attacks against Mobile Ad-Hoc Routing Protocols”, Technical Report, Department of Computer Science, North Carolina State University, 2003.

[11] D. Djenouri, O. Mahmoudi, D.L. Jones, M. Merabti, “On Securing MANET Routing Protocol against Control Packet Dropping”, *Proceedings of IEEE International Conference on Pervasive Services*, pp. 100-108, 2007.

[12] Donald Welch, “Wireless Security Threat Taxonomy”, *Proceedings of IEEE Workshop on Information Assurance*, pp. 261-265, 2003.

[13] C. Logeshwari and N. Gugha Priya, “Enhancing the Performance of MANETs using Period based Defense Mechanism”, *Proceedings of International Conference on Simulations in Computing*, pp. 174-182, 2014.

[14] S. Kavitha and E. Bharathi, “Reduction of Overhead Caused by Enhanced Adaptive Acknowledgement with Broadcast Algorithm for Mobile Ad-Hoc Networks”, *International Journal of Computer Science and Technology*, Vol. 5, No. 1, pp. 79-83, 2014.

[15] Shraddha Kamble, B.K Mishra and Rajesh Bansode, “Performance Enhancement of Intrusion Detection System Using Advance Adaptive EAACK for MANETs”, *International Journal of Computational Engineering Research*, Vol. 6, No. 6, pp. 45-52, 2016.

[16] Saima Zafar, Hina Tariq and Kanza Manzoor, “Throughput and Delay Analysis of AODV, DSDV and DSR Routing Protocols in Mobile Ad Hoc Networks”, *International Journal of Computer Networks and Applications*, Vol. 3, No. 2, pp. 25-31, 2016.

[17] Neerja Khatri and Arvind Kumar, “Analysing Performance of AODV in MANET: A Survey”, *International Journal of Scientific and Engineering Research*, Vol. 3, No. 6, pp. 1-4, 2012.

[18] Vivek Soi and B.S. Dhaliwal, “Performance comparison of DSR and AODV Routing Protocol in Mobile Ad hoc Networks”, *International Journal of Computational Intelligence Research*, Vol. 13, No. 7, pp. 229-231, 2017.

[19] Osama S. Faragallah, “An Enhanced Chaotic Key-Based RC5 Block Cipher Adapted to Image Encryption”, *International Journal of Electronics*, Vol. 99, No. 7, pp. 925-943, 2012.

[20] K. Vijaya Kumar and K. Somasundaram, “A Symmetric Multiple Random Keys (SMRK) Model Cryptographic Algorithm”, *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 3, No. 11, pp. 10896-10903, 2015.

[21] Reena Chaudhary and Sunil Ahuja, “Implementing Cryptographic Algorithm in Term of Privacy in AODV Routing Protocol”, *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 6, No. 4, pp. 288-293, 2016.

[22] I.D. Chakeres and E.M. Belding Royer, “AODV Routing Protocol Implementation Design”, *Proceedings of International Workshop on Wireless Ad hoc Networking*, pp. 441-448, 2004.

[23] S. Capkun, L. Buttyan and J.P. Hubaux, “SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks”, *Proceedings of 1st ACM Workshop on Security of Ad hoc and Sensor Networks*, pp. 21-32, 2003.