International Journal of Scientific Research and Engineering Development-– Volume 4 Issue 2, Mar- Apr 2021

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

MANET with Trust Based Secure AOMDV

Reshma R*, John J Thanikkal**, Vidhun M***, Farsana Rasheed C****

*(Electrical and Electronics Engineering, IES College of Engineering, Chittilappilly , Kerala)
** (Electrical and Electronics Engineering, IES College of Engineering, Chittilappilly , Kerala)
*** (Electrical and Electronics Engineering, IES College of Engineering, Chittilappilly , Kerala)
**** (Electrical and Electronics Engineering, IES College of Engineering, Chittilappilly , Kerala)

****

Abstract:

A design of a protocol and the security of network in MANET is the vibrant research area for the past several years. In this paper we suggest a new method to provide reliable and secure data transmission in MANETs with under possible black hole attacks and Sybil attacks based on trust based multipath ad hoc on-demand multipath distance vector routing (T-AOMDV) protocol and homomorphic encryption scheme for security. Simulation results show the improvement of packet delivery ratio and network throughput, and decrement in network packet loss and delay in the presence of black hole nodes and sybil nodes in our proposed method.

Keywords — T-AOMDV, mobile adhoc network, homomorphic encryption, AODV, blackhole attack, sybil attack**.**

****

I. INTRODUCTION

The network of mobile devices which are infrastructure less and is continuously selfconfiguring that are connected wirelessly is known as Mobile Ad hoc Network (MANET). The devices in MANET changes its link to other devices regularly since the devices can move freely in any direction independently [1]. The vital performance factor which is essential in the Mobile Ad-hoc Network is the Routing protocol. Routing protocols in MANET are capable for handling a numerous number of nodes with restricted resources. Routing protocols broadcast information which choose the routes between any two nodes and specifies the route between the nodes in a network [2].

In MANET there are varieties of routing protocols. AODV and AOMDV are among them.The extension of AODV (Ad hoc on demand distance vector routing protocol) is the AOMDV (Ad hoc on demand multipath distance vector routing protocol) which is used for computing numerous loop free and link disjoint path. A list of the next-hops along with the corresponding hop counts are contained in the routing entries for each

destination**.** The sequence number is same for all the next hops and this helps in keeping track of a route. A node maintains the maximum hop count for all the paths (advertised hop count) for each destination and this advertised hop count is used for sending route advertisements of the destination.An alternate path to the destination is defined by each duplicate route advertisement received by a node.If the node has a less hop count than the advertised hop count for destination loop freedom is assured for that node by accepting alternate paths to destination. So, for the same sequence number there is no change in advertised hop count. The next-hop list and the advertised hop count are reinitialized when a route advertisement is received for a destination with a greater sequence number. For finding node-disjoint or link-disjoint routes AOMDV can be used [3].

There are different types of attacks in MANET. Black hole attack and Sybil attacks are among them.In networking, black holes refer to areas in the network where incoming or outgoing traffic is silently dropped,without notifying the source that the data did not reach its intended recipient [4]. The black holes themselves are invisible, and can only be detected by monitoring the lost traffic while examining the topology of the network hence it is known as black hole. A Sybil attack generates multiple numbers of identities from the same node which is malfunctioning. This type of attack is most dangerous to WSN because this type of attacks will also act as a gateway for several attacks such as wormhole and sinkhole etc. Encryption is the operation of altering information or data into a code in order to prevent the data from unauthorized access.There are different types of encryption techniques. Homomorphic encryption is among them.A kind of encryption where we can carry out operations on encrypted text and get encrypted result, which when decrypted would be same as you would get if operation was carried out on the decrypted text on first place is known as Homomorphicencryption [5].Based on the cooperation of nodes, a trust value is assigned to each node and its value gets updated continuously. In order to define a trust, route this value is used.

This paper provides reliable and secure data transmission in MANET using AOMDV protocol with Multipath trust management under possible black hole attack and Sybil attack is combined with homomorphic encryption scheme for security.

The rest of the paper is organized as follows. In section II, we present the related works.In section III, the proposed method is described. In section IV performance is evaluated.

II. RELATED WORKS

In this section we discuss other works related to MANET, routing attacks, AOMDV,trust mechanism and homomorphic encryption.

The infrastructure less network of mobile devices which is continuously self-configuring that are connected wirelessly is known as Mobile Ad hoc Network (MANET) [1]. In recent years, in the field of secured routing schemes MANETs have received increasing attention with focusing on data forwarding.Imrich Chlamtac et al. attempts to provide a complete overview of MANET [6]. MANETs plays an important role in the evolution of future wireless technologies. Then, theyreview the latest research activities in MANETs, including a summary of its characteristics, capabilities, applications and design constraints. A MANET is exposed to many types of attacks. P NarendraRedd et al.analysed the current state of- the-art of routing attacks and solutions in a MANET [9]. For solutions, they identified their advantages as well as their drawbacks. Their studies showed that although many solutions have been proposed, still they arenot perfect in terms of tradeoffs between effectiveness and efficiency. For example, some solutions that rely on cryptography and key management seem promising but they are high expensive for resource-constrained MANETs. Although some countermeasures work well in the presence of one attacker node but they might not be applicable in the presence of multiple colluding attackers. Some solutions may require some

modification to the existing protocol or a special hardware such as a GPS. Harsh Pratap Singh et al. presents a review of different protection mechanism to eliminate the blackhole attack from the network[8]. One of the serious threats in mobile ad hoc networkis black hole attacks. It influences the performance of the different routing protocol such as AODV by inserting a false route reply message and it also increases the network traffic.Mahesh K. Marina, et al. developed an on-demand, multipath distance vector protocol for mobile ad hoc networks[10]. Specifically, they proposed multipath extensions to a well-studied single path routing protocol known as Ad hoc Ondemand Distance Vector (AODV) referred to as Ad hoc on- demand Multipath Distance Vector (AOMDV). The protocol figures multiple loop-free and link-disjoint paths.Elbasher et al. define a new method to provide secured and reliable data transmission with black hole attack in MANET based on AOMDV protocol [7].Ch. Niranjan Kumar at all explained the Sybil attack and position verificationbased mechanism for the detection of Sybil node in Wireless Ad-hoc Networks[11]. After detecting the Sybil node,they block the node to mitigate the attack.Youssef Gahi1, et al. proposed a method to avoid forwarding packets over untrustworthy paths [12]. With this approach, each node evaluates itsneighbours to elect the ones that it will collaborate with. Based on its cooperation a trust value is assigned to each node. This value is updated continuously. These values are then used to define a trust route. Also, they provide protective measure that can preserve the privacy of nodes without degrading the robustness in performance. For that they utilize the concept of Fully Homomorphic Encryption and Multi-hop Homomorphic to achieve their goal. The Fully Homomorphic Encryption (FHE) is a powerful concept that can enable the operation of encrypted data in a blind fashion. FHE schemes allow performing algebraic computations unlike other schemes which support only a single type of operations. A kind of encryption where we can carry out operations on encrypted text and get encrypted result, which when decrypted would be same as you would get if operation was carried out on the decrypted text on first place is known as Homomorphic encryption[5].

III. PROPOSED METHOD

The infrastructure less network of mobile devices which is continuously self-configuring that are connected wirelessly is known as Mobile Ad hoc Network (MANET) [1]. In our proposed method MANET is constructed with AOMDV protocol.AOMDV is the multipath extension of AODV which establishes routes on demand. It uses multihop routing and is based on distance vector concept. AOMDV protocol consist of hello message, RREQ, RREP and error message (RERR).In order to identify the network, Source node send hello message to all other neighbouring nodes. After thatsource node broadcast RREQ as a route discovery process to find destination. If destination node receives RREQ message it will start RREPand send RREP message to the source node through the reverse path.When intermediate node receives duplicate RREP message it will send a REER message to node that transferred RREP message and path will break.

Trust is added to the AOMDV which gives TAOMDV. Trust factor is related to node movement and packets monitoring. Based on the degree of faithfulness and nodes involvement, routing functionality selects the node.ie. According to the preservation of packets, availability of nodes and level of successful packet transfer, a trust value is assigned to each node. If a node has highest trust value, it is selected as a part of trusted path over a period of time and this trusted path is used for packet transfer.

After that black hole and sybil attacks are constructed in MANET**.** Black-hole is defined as an attack created by an outside environment on a subset of the nodes in a network. The nodes are affected and modified by the adversary such that they do not transfer the information. These occupies the information which are created by the nodes are forwarded. The re-programmed nodes are termed as black hole nodes and that certain

region is called black hole region. Black holes are invisible by themselves in the topology of a network and by monitoring the lost traffic is the only way for detecting the black holes.

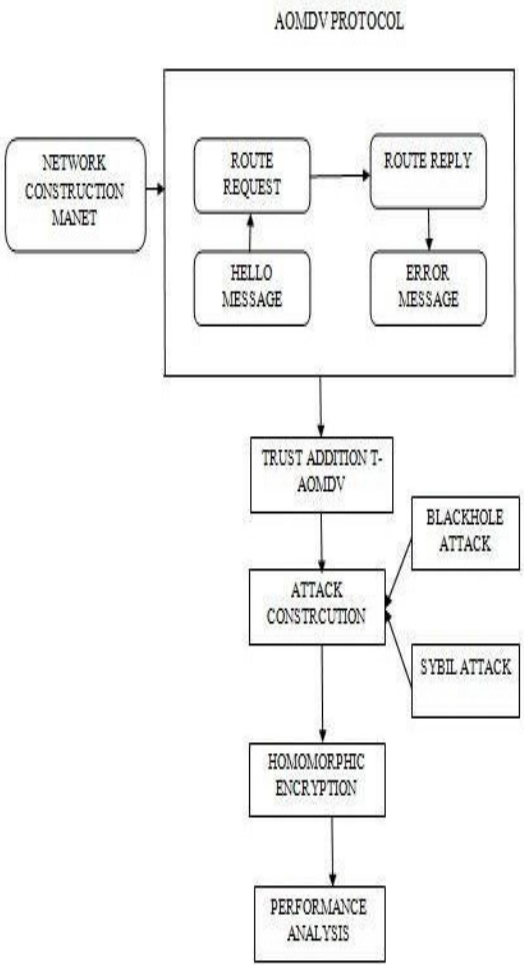

Fig 1: Flow diagram

A Sybil attack generates multiple numbers of identities from the same node which is malfunctioning. This type of attack is most dangerous to WSN because this type of attacks will also act as a gateway for several attacks such as wormhole and sinkhole etc. The way to create the Sybil attacker is during the process of communication node communicates with the other through one hop method. In that condition any node gets the access of the other normal node and it is the easy way to get the data from the nodes such as node position and id etc. By the use of this data the attacker node will create similar ids to establish the attacks to the normal nodes.

The message is encrypted using homomorphic encryption [HE] for giving security to the packet we are going to transfer.Homomorphic encryption allows complicated mathematical operations to be performed on encrypted data without adjusting the encryption.ie, If X wants to add 1 and 2, but X does not know how to add numbers. So, X asks Y to add those numbers also X does not trust Y. So, X encrypts numbers 1 and 2 into another numbers 33 and 54 and sent to Y. So, Y finds the sum of 33 and 54 and return 87 to X (Y has only access to encrypted data). Then X decrypts the 87 and finds the answer 3. After that performance is analysed. Flow diagram of proposed scheme is shown in fig 1.

IV. SIMULATION RESULTS

A. Simulation Metrics

In our project NS 2.34 is used as the simulation tool. We provide reliable and secure data transmission in MANETs with under possible black hole attacks and sybil attacks based on trust based multipath ad hoc on-demand multipath distance vector routing (TAOMDV) protocol and homomorphic encryption scheme for security. We define 50 nodes for our simulation among them node 6 and 12 are used as blackhole as well as sybilnodes, node 0 as sink node,node 1 as access point (monitoring node) and node 2,3,4 as cluster heads and all other nodes are child nodes or normal nodes. In our simulation normal node send data to cluster heads and cluster head send data to sink node. For the evaluation of our proposed scheme we simulated original AOMDV protocol (red), AOMDV with homomorphic encryption (green), and trust based AOMDV with sybil attack (pink) and black hole

attack (blue) with homomorphic encryption in the following metrics:

- Packet delivery ratio (%) :- total delivered packets by total sent packets
- Throughput (kbps) :- amount of data successfully received at destination per second
- Packet loss (%):- no: of lost packets during the data transmission process
- End to end delay (ms) :- receiving time – sending time
- Energy consumption (nJ) :- total energy consumed
- Routing overhead (RREQ packets) :- amount of additional packet injected into the network

B. Packet Delivery Ratio (PDR)

PDR is the ratio of total delivered packets by total sent packets. Refer to Fig. 2. Here, we can see that the packet delivery ratio (PDR) is compared with normal AOMDV with AOMDV with homomorphic encryption and our proposed scheme with blackhole and sybil attackers. We can observe that within the presence of blackhole nodes and Sybil nodes, the packet delivery ratio reduces in normal AOMDV and increases in AOMDV with homomorphic encryption. As seen, the proposed system has shown better performance in PDR compared to other methods.

PDR Simulation time vs. PDR

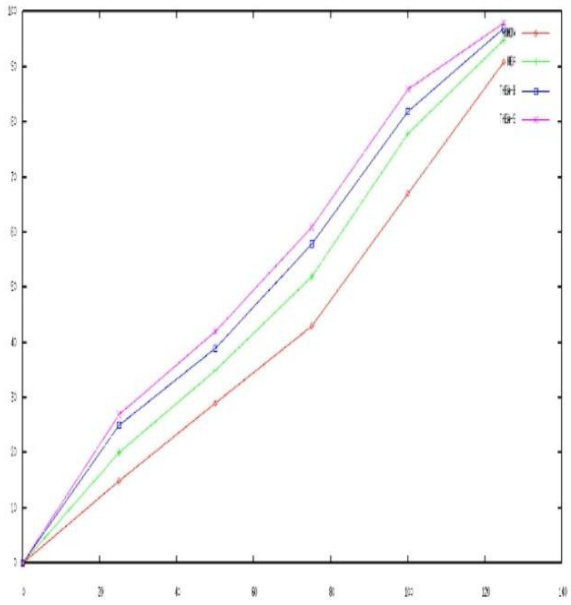

Fig.2:Packet delivery ratio

C. Throughput

Throughput is the amount of data successfully received at destination per second. Refer to Fig. 3. Here, we can see that the throughput is compared with normal AOMDV with AOMDV with homomorphic encryption and our proposed scheme with blackhole and sybil attackers.We can observe that within the presence of blackhole nodes and Sybil nodes, the throughput reduces in normal AOMDV and increases in AOMDV with homomorphic encryption. As seen, the proposed system has shown better performance in throughput compared to other methods.

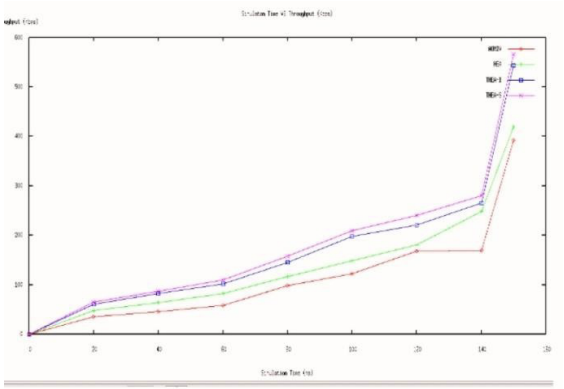

Fig 3:Throughput

D. Packet Loss

Packet loss is the no: of lost packets during the data transmission process. Refer to Fig. 4. Here, we can see that the packet loss is compared with normal AOMDV with AOMDV with homomorphic encryption and our proposed scheme with blackhole and sybil attackers. We can observe that within the presence of blackhole nodes and Sybil nodes, the packet loss is very high in normal AOMDV and decreases in AOMDV with homomorphic encryption. As seen, the proposed system has shown better performance in packet loss compared to other methods.

Loss Simulation time vs. loss

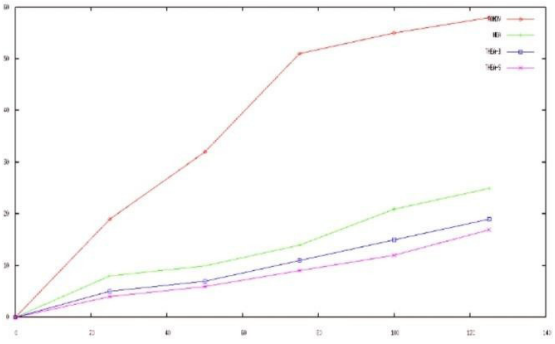

Fig.4:Packet loss

E. End to End Delay

Refer to Fig. 5. Here, we can see that the end to end delay is compared with normal AOMDV with AOMDV with homomorphic encryption and our proposed scheme with blackhole and sybil attackers. We can observe that within the presence of blackhole nodes and Sybil nodes, the end to end delay is very high in normal AOMDV and decreases in AOMDV with homomorphic encryption. As seen, the proposed system has shown better performance in end to end delaycompared to other methods.

End-End delay simulation time vs.End-End delay

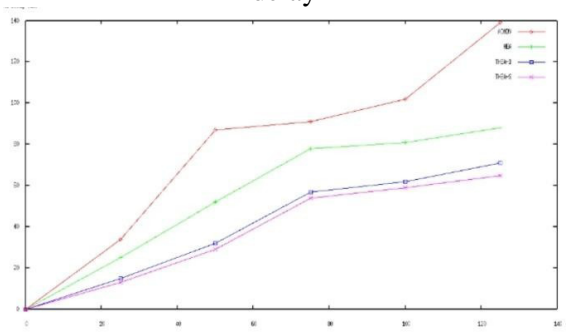

Fig.5: End-End delay

F. Energy consumption

A node consumes a particular amount of energy for every packet transmitted and every packet received. Refer to Fig. 6. Here, we compared the energy consumption for normal AOMDV with AOMDV with homomorphic encryption and our proposed scheme with blackhole and sybil attackers.We can observe that within the presence of blackhole nodes and Sybil nodes, theenergy consumption is very high in normal AOMDV and decreases in AOMDV with homomorphic encryption. As seen, the proposed system has shown better performance in energy consumption compared to other methods.

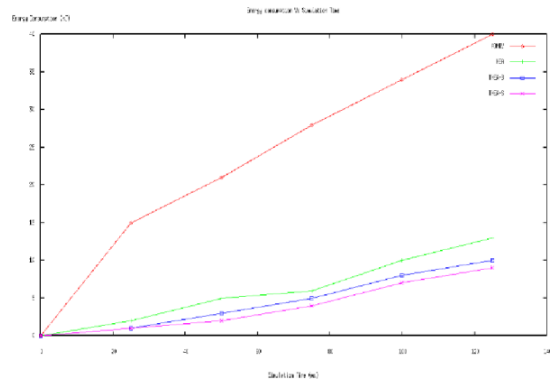

Fig 6: Energy consumption

G. Routing Overhead

Routing overhead is the amount of additional packet injected into the network. Refer to Fig. 7. Here, we compared the routing overhead for normal AOMDV with AOMDV with homomorphic encryption and our proposed scheme with blackhole and sybil attackers. We can observe that within the presence of blackhole nodes and Sybil nodes, the routing overhead is very high in normal AOMDV and decreases in AOMDV with homomorphic encryption. As seen, the proposed system has shown better performance in routing overhead compared to other methods**.**

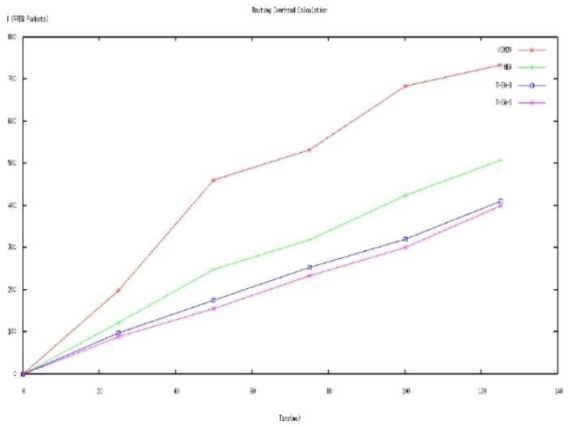

Fig.7: Routing overhead

V. CONCLUSION

In this paper we suggest a new method to provide reliable and secure data transmission in MANETs with under possible black hole attacks and Sybil attacks based on trust based multipath ad hoc ondemand multipath distance vector routing (TAOMDV) protocol and homomorphic encryption scheme for security. Due to the activities of the attackers' large number of packet loss, increased delay and reduced throughput occurs. Simulation results show that the increment in packet delivery ratio and network throughput, and decrement in network packet loss, energy consumption, routing overhead and delay in our proposed method with blackhole and sybil attackers. Since blackhole attack is more complicated than sybil, overall performance of proposed scheme under blackhole is less compared to sybil.

REFERENCES

[1] Wikipediawebsite. [online]. Available: https://en.wikipedia.org/wiki/Mobile_ad_hoc_network

[2] Sachin Lalar and Arun Kumar Yadav, "Comparative study of routing protocols in MANET", ISSN, 22 March ,2017

[3] Smita Singh, Shradha Singh,Soniya jain,S.R. Biradar, "Comparison and Study of AOMDV and DSDV Routing Protocols in MANET Using NS-2", IJCSE, 2012 [4] Wikipediawebsite. [online]. Available: https://en.wikipedia.org/wiki/black_hole_(networking)

[4] Quora website [online]. Available:https://www.quora.com/How-does-fullyhomomorphic-encryption-really-work

[5] Imrich Chlamtac, Marcoconti and Jennifer j-n Liu, "Mobile Ad Hoc Networking: Imperatives and Challenges, Ad Hoc Networks", vol. 1, no. 1, pp. 13-64, July, 2003

[6] Elbasher Elmadhi, Seong Moo Yoo, Kumar Sharshembiev, "Securing Data Forwarding Against Back Hole Attack in Mobile Ad Hoc Networks",IEEE, 2018 .

[7] Harsh PratapSingh, Virendra pal Singh,Rashmi Singh, "Cooperative blackhole/ greyhole attack detection and prevention in mobile ad hoc network: a review", International Journal of Computer Applications (0975 – 8887) volume 64– no.3, February, 2013 .

[8] P. Narendra Reddy, CH. Vishnuvardhan, V. Ramesh, "Routing Attacks in Mobile Ad Hoc Networks", International Journal of Computer Science and Mobile Computing,2013 .

[9] Mahesh K. Marina, Samir R. Das, "On-Demand Multipath Distance Vector Routing In Ad Hoc Networks", IEEE, .2001

[10] C H. Niranjan Kumar, Satyanarayana, "Detection of Sybil Attack Using Position Verification Method in Manets", International Journal of Modern Trends in Engineering and Research,2014.

[11] Youssef Gahi1, MouhcineGuennoun, ZouhairGuennoun, Khalil El-Khatib, "An Encrypted Trust-Based Routing Protocol", IEEE,2012 .

