International Journal of Computer Trends and Technology
ISSN: 2231-2803 / https://doi.org/10.14445/22312803/IJCTT-V67I4P110
Volume 67 Issue 4, 44-48, April 2019

Original Article

Trust-Based Secure AOMDV with Homomorphic Encryption for Multi-Path Mobile ADHOC Network

Farsana Rasheed C[1], Satheesh N Kaimal[2]

[1,2] *Electronics and Communication Engineering, A P J Abdul Kalam Technological University*
Thejus Engineering College, Kerala, India

Abstract *- A design of a protocol and the network's security in MANET has been a vibrant research area for the past several years. This paper suggests a new method for reliable and secure data transmission in MANETs under possible black hole attacks and Sybil attacks based on a trust-based, ad hoc on-demand multipath distance vector routing (T-AOMDV) protocol 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 that are infrastructure-less and continuously self-configuring, connected wirelessly, is known as Mobile Ad hoc Network (MANET). The devices in MANET change their link to other devices regularly since they can move freely in any direction independently [1]. The vital performance factor essential in the Mobile Ad-hoc Network is the Routing protocol. Routing protocols in MANET are capable of handling several nodes with restricted resources. Routing protocols broadcast information that chooses 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) used for computing numerous loop-free and link disjoint paths. A list of the next hops and the corresponding hop counts are contained in the routing entries for each destination**.** The sequence number is the same for all the next hops, which helps keep 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. Each duplicate route advertisement a node receives defines an alternate path to the destination. If the node has a less hop count than the advertised hop count for the destination loop, freedom is assured for that node by accepting alternate paths to the destination. So, there is no change in the advertised hop count for the same sequence number. 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. Blackhole attacks 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 network's topology; hence it is known as a black hole. A Sybil attack generates multiple numbers of identities from the same node, malfunctioning. This type of attack is most dangerous to WSN because this type of attack will also act as a gateway for several attacks such as wormholes and sinkholes etc. Encryption is altering information or data into a code 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 an encrypted result, which would be the same as you would get if an operation were carried out on the decrypted text in the 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. 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. Sybil attack is combined with a 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

This section discusses other works related to MANET, routing attacks, AOMDV, trust mechanisms, and homomorphic encryption.

The infrastructure-less network of mobile devices that is continuously self-configuring and connected wirelessly is known as Mobile Ad hoc Network (MANET) [1]. In recent years, MANETs have received increasing attention by focusing on data forwarding in secured routing schemes. Imrich Chlamtac et al. attempt to provide a complete overview of MANET [6]. MANETs play an important role in the evolution of future wireless technologies. Then, they review 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. analyzed the current state-of-the-art 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, they are still not perfect in trade-offs between effectiveness and efficiency. For example, some solutions that rely on cryptography and key management seem promising, but they are highly expensive for resource-constrained MANETs. Although some countermeasures work well in the presence of one attacker node, they might not apply to multiple colluding attackers. Some solutions may require modification to the existing protocol or special hardware such as a GPS. Harsh Pratap Singh et al. present a review of different protection mechanisms to eliminate the network's blackhole attack [8]. One of the serious threats in mobile ad hoc networks is black hole attacks. It influences the performance of the different routing protocols such as AODV by inserting a false route reply message, increasing 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 On-demand 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 the AOMDV protocol [7]. Ch. Niranjan Kumar et al.explained the Sybil attack and position verification-based mechanism for detecting Sybil nodes in Wireless Ad-hoc Networks[11]. They block the node after detecting the Sybil 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 its neighbors to select the ones 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 a protective measure that can preserve the privacy of nodes without degrading the robustness in performance. They utilize the concept of Fully Homomorphic Encryption and Multi-hop Homomorphic to achieve their goal. Fully Homomorphic Encryption (FHE) is a powerful concept that can enable the operation of encrypted data blindly. FHE schemes allow performing algebraic computations, unlike other schemes which support only a single type of operation. A kind of encryption where we can carry out operations on encrypted text and get the encrypted result, which, when decrypted, would be the same as you would get if an operation were carried out on the decrypted text in the first place, known as Homomorphic encryption[5].

III.PROPOSED METHOD

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

Trust is added to the AOMDV, which gives TAOMDV. The trust factor is related to node movement and packet monitoring. The routing functionality selects the node based on the degree of faithfulness and node involvement, and routing functionality selects the node. ie. According to the preservation of packets, availability of nodes, and level of the successful packet transfer, a trust value is assigned to each node. If a node has the highest trust value, it is selected as a part of the trusted path over time and used for packet transfer. After that, black holes 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 occupy the information which is created by the nodes and are forwarded. The re-

programmed nodes are termed black hole nodes, and that certain region is called the black hole region. Black holes are invisible in the topology of a network, and monitoring the lost traffic is the only way to detect the black holes.

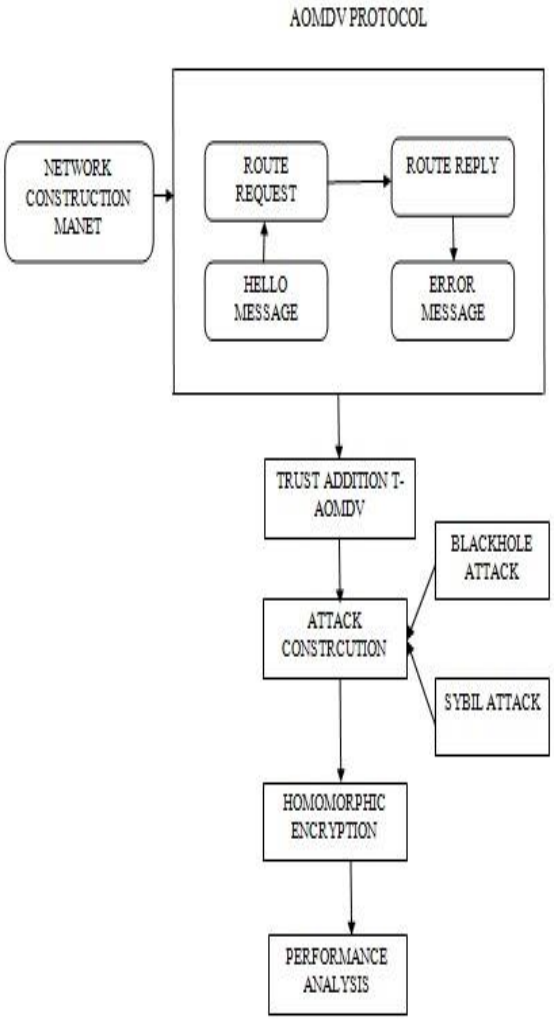

Fig. 1 Flow diagram

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

The message is encrypted using homomorphic encryption [HE] to give security to the packet we will transfer. Homomorphic encryption allows complicated mathematical operations on encrypted data without adjusting the encryption. 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 numbers 33 and 54 and sent to Y. So, Y finds the sum of 33 and 54 and returns 87 to X (Y has only access to encrypted data). Then X decrypts the 87 and finds the answer 3. After that, performance is analyzed. The flow diagram of the 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 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. We define 50 nodes for our simulation. Nodes 6 and 12 are used as blackholes, Sybil Noyes, node 0 as sink node, node 1 as an access point (monitoring node), node 2,3,4 as cluster heads, and all other nodes are a child or normal nodes. In our simulation, the normal node sends data to cluster heads, and the cluster head sends data to the sink node. For the evaluation of our proposed scheme, we simulated the 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):- the 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):- the number of additional packets injected into the network.

B. Packet Delivery Ratio (PDR)

PDR is the ratio of total delivered packets to 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 black hole nodes and Sybil nodes, the packet delivery ratio reduces in normal AOMDV and increases in AOMDV with homomorphic encryption. The proposed system has shown better PDR performance than other methods.

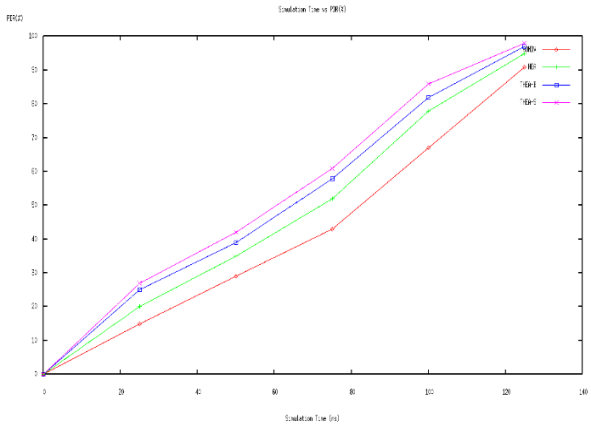

Fig. 2 Packet delivery ratio

C. Throughput

Throughput is the amount of data successfully received at the 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 the throughput reduces in normal AOMDV and increases in AOMDV with homomorphic encryption within the presence of black hole nodes and Sybil nodes. The proposed system has shown better throughput performance than other methods.

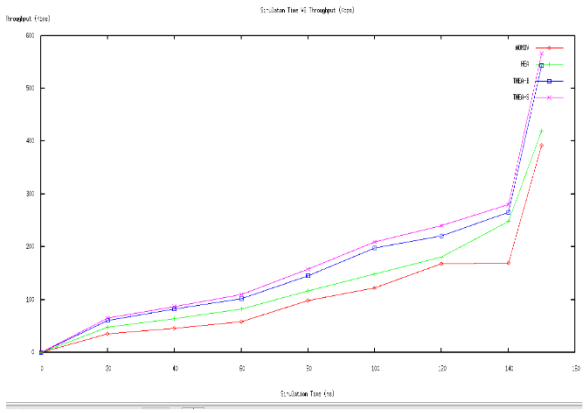

Fig. 3 Throughput

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 the packet loss is very high in normal AOMDV and decreases in AOMDV with homomorphic encryption within the presence of black hole nodes and Sybil nodes. As seen, the proposed system has shown better performance in packet loss compared to other methods.

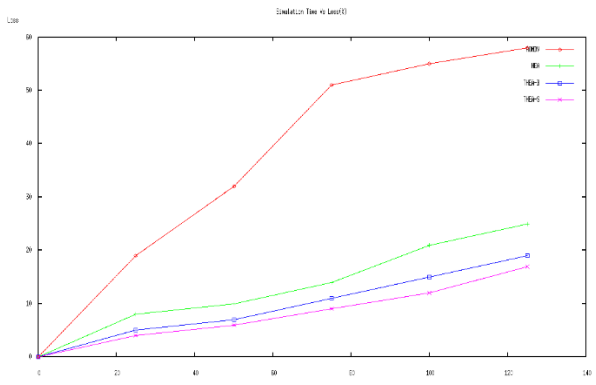

Fig. 4 Packet loss

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 the end-to-end delay is very high in normal AOMDV and decreases in AOMDV with homomorphic encryption within the presence of black hole nodes and Sybil nodes. The proposed system has shown better performance in the end-to-end delay than other methods.

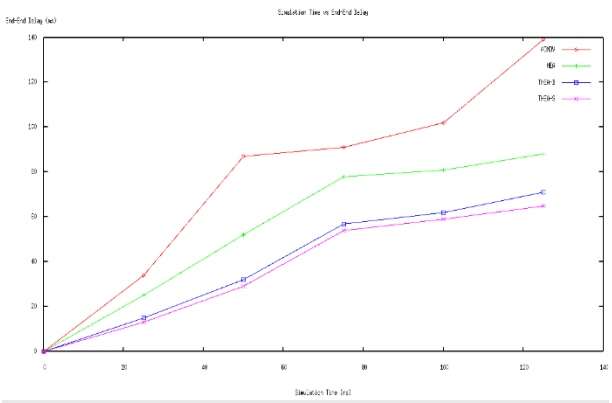

Fig. 5 End to end delay

F. Energy Consumption

A node consumes a particular amount of energy for every packet transmitted and 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 black hole nodes and Sybil nodes, the energy consumption is very high in normal AOMDV and decreases in AOMDV with homomorphic encryption. As seen, the proposed system has shown better energy consumption performance than other methods.

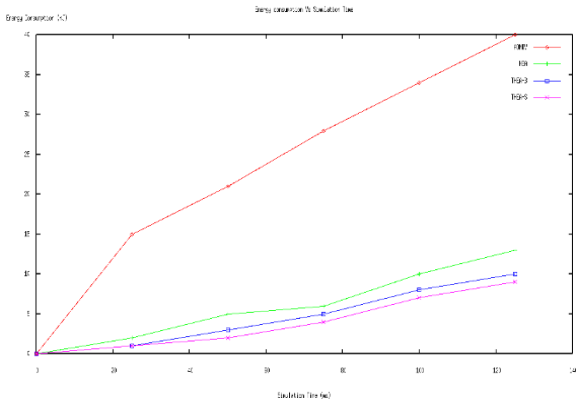

Fig. 6 Energy consumption

G. Routing Overhead

Routing overhead is the number of additional packets injected into the network. Refer to Fig. 7. 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 black hole nodes and Sybil nodes, the routing overhead is very high in normal AOMDV and decreases in AOMDV with homomorphic encryption. The proposed system has shown better performance in routing overhead compared to other methods**.**

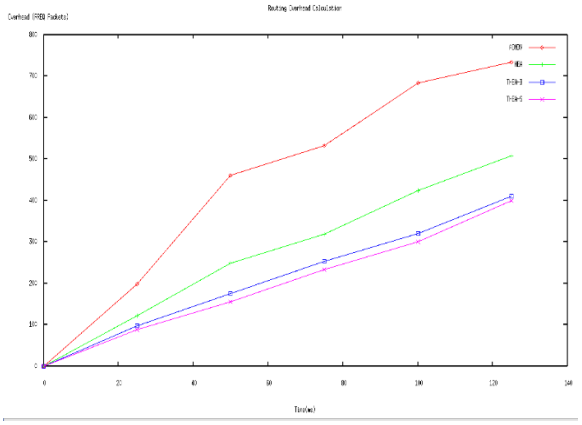

Fig.7 Routing overhead

V. CONCLUSION

This paper suggests a new method for reliable and secure data transmission in MANETs under possible black hole attacks and Sybil attacks based on a trust-based, ad hoc on-demand multipath distance vector routing (T-AOMDV) protocol homomorphic encryption scheme for security. Due to the attackers' large number of packet loss activities, increased delay and reduced throughput occur. Simulation results show the packet delivery ratio and network throughput increment and decrement in network packet loss, energy consumption, routing overhead, and delay in our proposed method with blackhole and Sybil attackers. Since the black hole attack is more complicated than Sybil, the overall performance of the proposed scheme under the black hole is less than Sybil.

REFERENCES

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

[2] Sachin Lollar 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] Wikipedia website. [online]. Available: https://en.wikipedia.org/wiki/black_hole_(networking).

[5] Quora website [online]. Available:https://www.quora.com/How-does-fully-homomorphic-encryption-really-work

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

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

[8] Harsh Pratap Singh, 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.

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

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

[11] 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

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