Journal of Information Security and Applications 51 (2020) 102425

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Secure and reliable data forwarding using homomorphic encryption against blackhole attacks in mobile ad hoc networks

Elbasher Elmahdi, Seong-Moo Yoo*, Kumar Sharshembiev

Electrical and Computer Enginreering, The University of Alabama in Huntsville, 301 Sparkman Dr NW, Huntsville, AL 35899, USA

ARTICLE INFO

Keywords:
Mobile ad hoc network security
Secure message transmission
Blackhole attack

ABSTRACT

A mobile ad hoc network (MANET) is a dynamic wireless network without any infrastructures. It is vulnerable to many types of attacks. Thus, security has turned out to be an important factor to facilitate secured communication between mobile nodes in a wireless environment. Recently, many routing protocols have been established. But most of them do not consider the security criteria in their designing. So, practically any node can maliciously disrupt communication of other nodes. Hence, a new approach is proposed in this paper to provide reliable and secure data transmission in MANETs under possible blackhole attacks based on modified ad-hoc on-demand multipath distance vector (AOMDV) protocol. We divide the message into multiple paths to the destination and use homomorphic encryption scheme for cryptography technique. The performance of the proposed scheme is stable with very high packet delivery ratio while that of AOMDV is found to be vulnerable with the intrusion of malicious nodes in the network. Simulation results show that, compared to the original AOMDV scheme, our proposed scheme improves considerably the packet delivery ratio and network throughput in the presence of malicious nodes.

1. Introduction

Each node in a mobile ad hoc network (MANET) is mobile, so the node can join the network, while at the same time other nodes leave it or fail to connect because they move to a region that is not in the covering range of the network. Here, each node involves in operations such as route discovery or data forwarding in the network. For this purpose, multiple routing protocols have been proposed. Most of the protocols focus on two types of routing algorithms: the table-driven type (the proactive type) and the on-demand type (the reactive type) like AODV, DSDV, DSR, or even multipath protocols like AOMDV according to the way of discovering and maintaining the routes [1]. Since data forwarding is dependent on each intermediate node, securing data transmission is an important issue [2].

The security in MANETs has become an active area of research, especially for applications such as emergency operations, military applications, vehicular applications, etc. [3]. In such an environment, malicious or selfish nodes can disrupt or even deny the communications of any node within the networking domain. In MANETs every node in the network is required to assist in the network establishment, its maintenance, and the network operation. In MANETs unique techniques define the network environment such as network topology is continuously changed, storage is limited, wireless links are not secure, and there exist many limitations [4]. Due to MANET's inherent characteristics mentioned above, it is necessary to save or secure data transmission to achieve effective communication in MANETs because most of the routing protocols proposed for MANET's assume a trusted and reliable environment and they do not consider the security issues in their initial designs.

The communication in MANETs includes two phases, the route discovery phase and the data transmission phase, and both phases are vulnerable to a variety of attacks. In the first phase, adversaries can disrupt the route discovery by impersonating the destination, responding with stale routing information, or by distributing fake control traffic. However, adversaries can also disrupt the data transmission phase and, thus, incur significant data loss by tampering with, falsely redirecting, or even dropping data traffic [5]. To provide comprehensive security in MANETs, both phases of communication must be protected.

In this paper, our concern is secure data transmission by assuming that routes are already established from a sender to a receiver. Our proposed scheme is based on ad hoc on-demand multipath distance vector (AOMDV) protocol for discovering active transmission paths. We have investigated the security of AOMDV protocol, a multipath extension of the Ad hoc On-Demand Distance Vector (AODV) routing protocol against blackhole attacks. After discover-

* Corresponding author.
E-mail address: yoos@eng.uah.edu (S.-M. Yoo).

https://doi.org/10.1016/j.jisa.2019.102425
2214-2126/

ing the routes between a source and a destination node, a message is divided into many parts and each part is encrypted using Enhanced Homomorphic Cryptosystem (EHC) [3, 20] before the sender transmits a part of the message to the destination [3]. Here, malicious nodes may be contained in the route and may make blackhole attacks. The problem of the attacks in the AOMDV protocol is addressed in this paper. So, our scheme is not an intrusion detection or intrusion isolation system, but it is an intrusion avoidance system from malicious nodes.

The idea of this scheme is to assign a set of disjoint paths into a set of groups and several active disjoint paths are assigned to each group, where all disjoint paths are connected between a sender and a receiver. We divide a message into many parts before the message is transmitted, and encrypt each part based on homomorphic encryption scheme. Then, the part of the message is transmitted to each group in order that only one encrypted part of the message is able to reach each group. Every node in each group can receive the same part of the message. Then, even if a part of the message is dropped, the part of the message can be delivered to the destination through another safe path. Thus, the receiver is able to receive the whole encrypted parts of the message, combine them, decrypt the whole parts, and recover the whole message.

We organize this paper as follows. Sections 2 explains closely related work. Section 3 introduces methodology. The problem to be solved in this paper is mentioned in Section 4. Our proposed scheme is described in Section 5. Section 6 analyzes our analytical model. Section 7 shows the simulation results. Conclusion with future work is mentioned in Section 8.

2. Related work

In this section, previous methods to secure data forwarding in MANETs are explained. Securing the data forwarding has received relatively less interest in works, although several proposals have handed out with the problem of secure ad hoc routing. Previous studies of protecting the data forwarding can be classified into three categories: information spread with end-to-end security, localized collaboration and information cross-validation, and applying cryptographic primitives.

2.1. Information spread with end-to-end security

Some previous studies of protecting the data forwarding based on information spread with end-to-end security. The main idea of information spread with end-to-end security is to defend the data transmission against the malicious behavior of other nodes. It provides further protection to secret messages from being compromised when they are delivered across the insecure network. It is based on information spread and end-to-end security. Papadimitratos and Haas [5] proposed secure data transmission scheme in MANETs. It operates just in an end-to-end procedure, exploits the redundancy of multipath routing and adapts its operation to remain efficient and effective even in highly adverse environments. It operates without limited intuition on the security associations and network trust and it affords the loss of data along with adjusting its operation to the network circumstances. Lou et al. [6] proposed a security protocol for reliable data delivery to enhance the data confidentiality service in a MANET. The basic idea in this scheme is to transform a secret message into multiple shares by secret sharing schemes and then deliver the shares via multiple independent paths to the destination so that even if a small number of nodes are compromised, the whole secret message is not compromised. The main problem of these schemes is that every node in the network needs to establish a security association with every other node in the network, thereby increasing overhead.

Wazid et al. [7–9] proposed a new efficient techniques for the detection and prevention of multiple attacker nodes in WSNs. In these techniques, the entire WSN is divided into several clusters and each cluster has a powerful high-end sensor node, which is called a cluster head and is responsible for the detection of attacker nodes, if present, in that cluster. Also, these techniques are suitable for the resource-constrained sensor nodes due to low computation and communication overheads. Satav et al. [10] proposed a technique to secure route selection in adverse environment in MANETs. The proposed approach added route reliability parameter in the routing table to categorize the paths as reliable or unreliable, but this addition increases the computational and storage overhead while reduces the packet delivery ratio and end to end delay. This proposal deals with security issues in route discovery stage, but our proposal deals with those in data transmission stage.

2.2. Localized collaboration and information cross-validation

The main idea of localized collaboration and information cross-validation is that local neighboring nodes collaboratively monitor and tolerate each other, while no single node is superior to the others. It exploits localized collaboration and information cross-validation to protect the network in a self-organized manner. Yang et al. [11] proposed self-organized network-layer security. It does not concern itself with any form of cryptographic security on the messages being routed. Instead, it covers the network from malicious nodes by detection and reaction to misbehaviors. It is a network-layer security solution that protects routing and forwarding operations in an integrated framework. The main problem with this scheme is that the energy consumption of this approach is too large.

2.3. Applying cryptographic primitives

Chinthanai et al. [12] proposed enhanced adaptive acknowledgment for intrusion detection. It uses a digital signature to prevent the attacker from fabricating acknowledgment packets. The scheme shows higher malicious-behavior-detection rates in certain situations while not affecting the network performances. Tan et al. [13] proposed a mechanism to secure data transmission using the AES cryptographic primitive with the underlying protocol as AODV. This scheme specifically targets the blackhole attacks with the importance of improving network parameters like throughput and packet delivery ratio. Ertaul et al. [14] used elliptic curve cryptography (ECC) and threshold cryptosystem (TC) to securely deliver message, splitting the message into a number of pieces before or after using ECC to encrypt them individually and sending them to the receiver. At the receiving side, each share of the secret is decrypted using ECC to get the original message. The main problem of the previous schemes produces additional routing overhead in cases of a well-informed adversary.

Sultana et al. [15] proposed a method to secure data packet in spite of blackhole attacks in MANETs through AOMDV routing protocol. ECC has been chosen to secure the packets against blackhole attacks. The main problem of this proposal is that it does not completely avoid blackhole attacks due to dropping the message even if it is encrypted. In addition, there exist some proposals generating automated mechanisms. They choose the alternate path automatically that will be reliable and secure. Also, Jain et al. [16] proposed an improved version of AODV routing protocol using homomorphic encryption scheme which prevents pollution attack and accomplishes in maintaining integrity security standard by following minimum hop count path. It allows an intermediate node to perform XOR operation on arriving data. The core technique involved in this technique is Message Authentication Code

(MAC) based on Universal Hash Function (UHF). However, minimum hop count path may lead to congestion in network. Rangasami et al. proposed a protocol [17] analyzing the usefulness and threats that will be faced by the service providers while taking up the homomorphic encryption schemes to provide confidentiality of data stored in cloud computing. From this study, they concluded that homomorphic encryption scheme paves a new way of securing data in cloud and it enables cloud service providers to serve the clients in a more efficient way by preserving the data confidentiality and integrity.

In summary, most of the previous work for securing AOMDV protocol in MANETs cannot avoid black hole attacks because an attack drops data even if it is encrypted. Our proposed scheme seems to be more reliable and secure to deliver the encrypted data to the destination.

3. Methodology

3.1. Ad hoc on-demand distance vector routing (AODV)

AODV is an on-demand distance vector routing protocol built on the DSDV algorithm [18]. Also, it is a reactive routing protocol which means routes are determined only when needed, and it is a single path and loop-free protocol. When a source has data to deliver it to a destination in an unknown position in the network, then it broadcasts a Route Request message (RREQ) to figure out that destination. In this case, when the route request is received by the intermediate node, a route is created to the destination. If the receiving node is not the destination node, has not received this RREQ previously, and does not have a route to the destination, it rebroadcasts the RREQ message again. But if the receiving node has a route to the destination or it is the destination, it creates a Route Reply message (RREP) to re-send it back to the source. After the source receives the RREP message, it maintains the route to the destination to utilize it for sending data to the destination. In case of multiple RREPs are received, then the route with the shortest path is chosen from the source. When data is flowing from the source to the destination and a route fail is recovered, a RERR is sent towards the source. When the source receives the RERR, it cancels the route and recovers another one if it needs it [19].

3.2. Ad hoc on-demand multipath distance vector routing (AOMDV)

The main objective of this paper is to provide a reliable and secure AOMDV routing protocol for the data transmission by means of our proposed scheme. AOMDV shares several characteristics with AODV, based on the distance vector concept. Moreover, AOMDV also finds routes on demand using a route discovery procedure in MANETs. The main difference is the number of routes found in each route discovery, which contributes to solve the problem of link failure in ad hoc networks. AOMDV provides efficient route switching when links break down between the nodes in the network by selecting another route from selected routes stored previously instead of initiating a route request process again. So, in comparison with AODV, AOMDV improves the performance in many aspects, such as the packet delivery ratio, end-to-end delay, and control overhead of the network [20].

3.3. Enhanced homomorphic cryptosystem (EHC)

Homomorphic encryption is the operation on the encrypted data which can offer the same results after calculations as the working straightly on the clear data. Homomorphic encryption schemes have the property of additive, multiplicative or mixed multiplicative homomorphism. In additive property, performing decryption on the sum of two ciphertexts is the same as addition of two plaintexts represented as $E(a + b) = E(a) + E(b)$. In multiplicative property, performing decryption on the product of two ciphertexts is the same as multiplication of the two plaintexts represented as $E(a * b) = E(a) * E(b)$. In mixed multiplicative property, performing decryption on the product of one ciphertext plaintext is the same as multiplication of two plaintexts, represented as $E(a * b) = E(a) * b$ [21].

In our proposed scheme, EHC [3, 20] is used as cryptographic algorithms based on additive homomorphic encryption. The general practical structure for the encryption and decryption scenario of EHC scheme is introduced below. This cryptosystem uses large number m, where $m = p \times q$. Here p and q are large prime numbers, which are kept secret. q is a sharing secret key. That number m is also a secret key to encrypt the data. Finding a random number r seems to be an extremely difficult problem because it will be generated randomly, which is kept secret. In principle, the EHC scheme consists of three main procedures: the key generation (**K**), the encryption algorithm (E) and the decryption algorithm (D), as illustrated below.

Secret Key Generation (K):

- $p,\ q\ \in\ P$, where P is prime, and $m = p * q$.
- Generate a random number r.
- The set of original plaintext messages $P = Zp = \{x:\ x\ <= p\}$, $Zm = \{x:\ x\ < m\}$ has the set of ciphertext messages.
- Secret values $r,\ m$ and q
- Shared Key $K = p$.

Encryption (E):

- $x\ \in\ Zp$
- The ciphertext C is calculated as $y = Ep(x) = (x + r \times pq)\,(mod\ m)$.

Decryption (D):

- The plaintext x is recovered as $x = Dp(y) = y\ mod\ p$.

4. Assumptions and problem statement

To deliver the message reliable and secure from the source to the destination, we propose a scheme explained in the next section. Before that, assumptions and problem statement are described here.

4.1. Assumptions

- In a MANET, there are a sender, a receiver and several dynamic nodes between them for forwarding the data.
- AOMDV protocol is used for the network layer to have a set of active disjoint paths between the sender and the receiver.
- A set of active disjoint paths after route discovery phase between the sender and the receiver in the standard multipath routing protocol AOMDV is modified as follows: While the source node starts route discovery to the destination, a proposed route count parameter is added in the routing table. This proposed parameter will count the active paths between source and destination in the routing table. After route discovery process, the source node checks routing table for available paths and its count {(next hop IP1, hop_count1), (next hop IP2, hop_count2), (next hop IP3, hop_count3), ...}. Then, the whole maintained paths in the routing table will be used to combine the transmitted parts of the message. Now the source sends the first part of the message through the two or more maintained routing paths which have the maximum sequence number or minimum hop count in case of the same sequence number in the routing table. The source also sends the second part of the

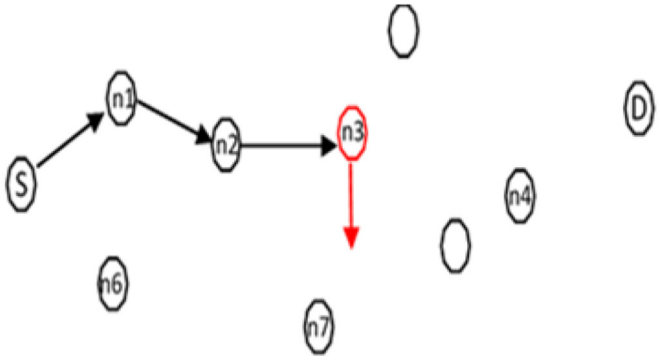

Fig. 1. Node S sends some packets to node D but node n3 drops all data packets.

message to the next two or more paths in the routing table, and so on until the last part of the message is sent.
- We also assume that the shared key p established from EHC is distributed between the sender and the receiver by using key distribution protocol Elliptic Curve Diffie Hellman (ECDH) algorithm [22].
- The message to be sent is a code which is recognized previously by both the sender and the receiver and is uploaded in their nodes.
- Malicious nodes (blackhole attackers) are included in the network. These nodes cooperate in route discovery phase and forward all control packets (such as route request, route error, route reply) correctly, but silently drops all data packets.
- All active paths in each group could be affected by malicious nodes after route discovery phase is completed.

4.2. Problem statement

In multipath routing protocols like AOMDV, assume that the source node selects the best route to forward packets to the destination node, which includes many malicious nodes. These malicious nodes, placed on the route, forward the control packets but drop all data packets. Refer to Fig. 1. Source node S sends packets to destination node D using route {S, n1, n2, n3, n4, D}. Here, node n3 is malicious and drops the entire data packets passing through it so they do not reach the destination node.

When the data transmission path includes blackhole attacker, data is not delivered to the destination as the attacker drops it. Also, when the entire data is sent via the single path without dividing it up and encryption, the attacker gains a complete knowledge about the data. The goal of the proposed scheme is to deliver and secure the entire message even if some disjoint paths are not working due to malicious nodes (blackhole attacks).

5. Proposed Scheme

In this section, the proposed scheme is introduced. First, we explain the procedure of the main idea, then a practical example of the proposed scheme.

5.1. Main idea

The proposed protocol is implemented by modifying the original protocol AOMDV as explained in the following and as shown in Fig. 2:

- A set of active disjoint paths n between a sender and a receiver are created. In our network topology, n is assumed as the number of active routes in the topology, and it is a fixed chosen value for creating multiple paths between a sender and a receiver to send a part of message. The sender routing table is prepared by adding all important details for the data routing into each selected path in the topology between the sender and the receiver.
- Combine these paths into groups G by dividing n by the desired number of paths in each group by assuming that not less than two active paths in each group $G = (n \,/\, 2\ or\ more)$.
- Before sending the message (code), the sender assigns a unique message ID (*msg-id*) to the entire message and divides it by the number of groups G for dismantling the entire message M/G, where M is the entire message and G is the number of groups of combined active disjoint paths.
- Moreover, each part of the entire message m is associated with a unique part message ID as (*msg-sp-id1, msg-sp-id2,...*,etc.) is used at the receiver side to gather the entire message again.
- Then, the sender encrypts all parts $m1$, $m2$, $m3$, ..., etc. of the entire message using EHC for getting $Ep(m1)$, $Ep(m2)$, $Ep(m3)$, ..., etc., where p is the secret key, and send them to the receiver along with *msg-id, msg-sp-id, msg-sp-id-sum* through active disjoint paths in each group, so each group will have only one encrypted part within the same message ID and message part ID.
- On the receiver side, to know the total number of encrypted parts of the entire message, we use the message part ID sum (*msg-sp-id-sum*) within the encrypted parts.
- The receiver recovers the whole message by adding up all encrypted parts of the entire message that has the same message ID using the additive property in homomorphic encryption scheme $Ep(m1) + Ep(m2) + Ep(m3)$, ..., etc. till reaching the message part IDs sum, *msg-sp-id-sum*.
- If the receiver gets a duplicate part of encrypted parts of the message which has the same message id and message part id, then it will discard the duplicated part.
- Finally, the receiver decrypts the sum of all the encrypted parts of the message using EHC, $X = Dp\,(Ep(m1) + Ep(m2) + Ep\,(m3)$, ..., etc.) to recover the original message M.

5.2. Example scenario

Refer to Fig. 3:

- The number of disjoint paths $n = 6$ between the sender and receiver.
- Number of groups () is

$$G = n \,/\, two\ or\ more\ paths\ in\ each\ group$$

$$G = 6 \,/\, 2 = 3$$

- The entire message $M = 9$.
- Parts of the entire message

$$m = M \,/\, G$$
$$= 9 \,/\, 3 = 3 \quad where\ m\ is\ m\ 1 = m2 = m3$$

- The message's id for the entire message M is $msg - id = 1$.
- The message part ids for the message parts are $msg - sp - id1 = 1$, $msg - sp - id2 = 2$, and $msg - sp - id3 = 3$.
- So, the message part id's sum is

$$msg - sp - id - sum = msg - sp - id1 + msg - sp - id2 + msg - sp - id3$$
$$= 1 + 2 + 3 = 6$$

- Encrypted the message parts $m1$,$m2$,$m3$ using EHC at the sender before sending them to the destination:

We have $M = 9$ and $m1 = m2 = m3 = 9/3 = 3$

Encryption process:

Select $p = 11, q = 7$ and $r\ (random) = 2$

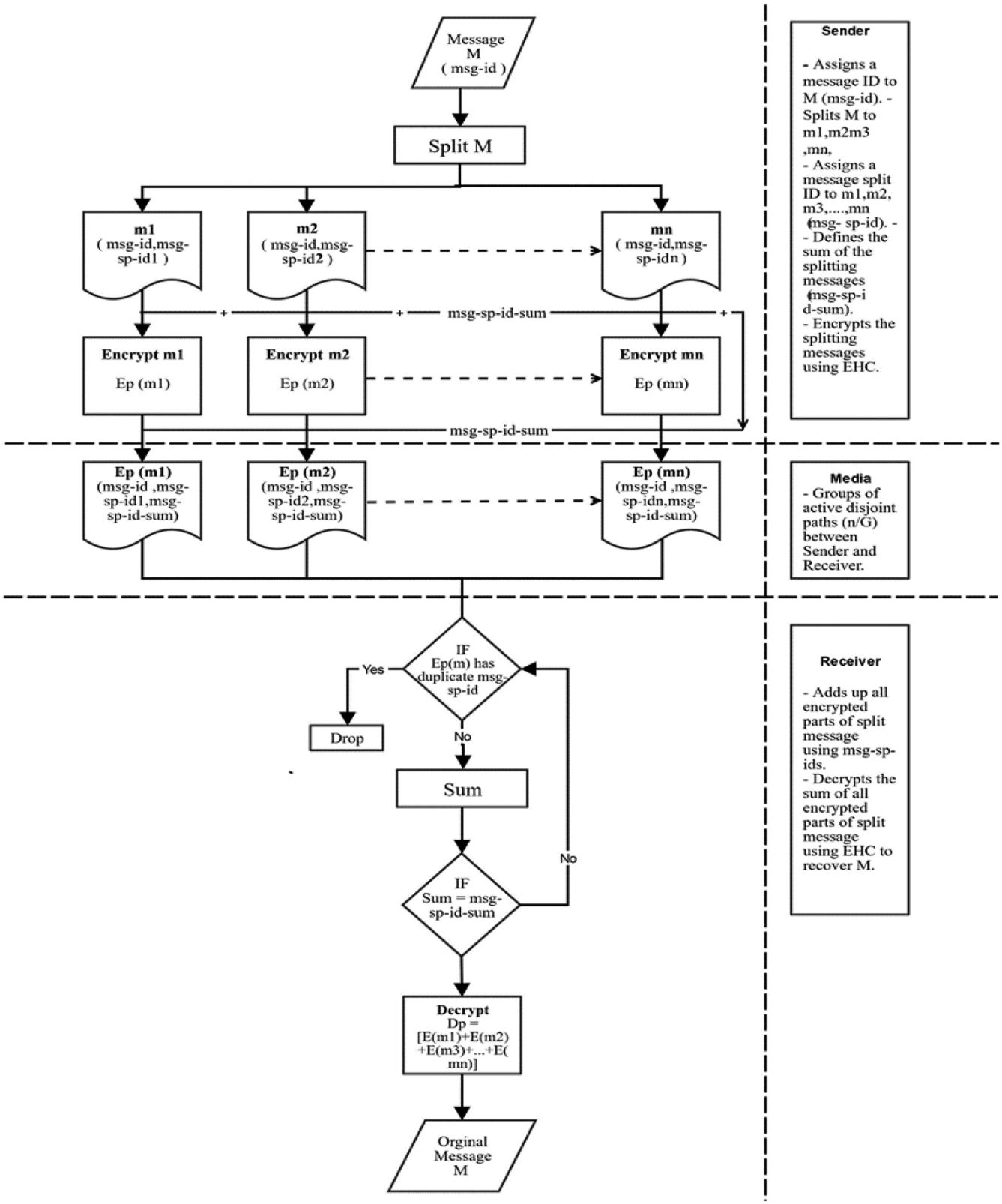

Fig. 2. The procedure of the proposed scheme.

Then $m = p \times q = 11 \times 7 = 77$

$$\boldsymbol{Ep}\ (\boldsymbol{m}1) = (\boldsymbol{m}1 + \boldsymbol{r} * \boldsymbol{pq})\ (\boldsymbol{mod}\ \boldsymbol{m})$$
$$= (3 + 2{*}117)\ (mod\ 77) Ep\ (m1) = 25$$

And so on for $m2$ and $m3$

$$Ep\ (m2) = 25\ and\ Ep\ (m3) = 25$$

- Sending Ep ($m1$) to group $G1$, Ep ($m2$) to group $G2$ and Ep ($m3$) to group $G3$ along with clear *msg-id*, *msg-sp-id*, and *msg-sp-id-sum* to be used to recover the entire message at the receiver side.
- On the receiver side, the receiver adds up all the encrypted parts of the entire message with the same $msg - id = 1$ by

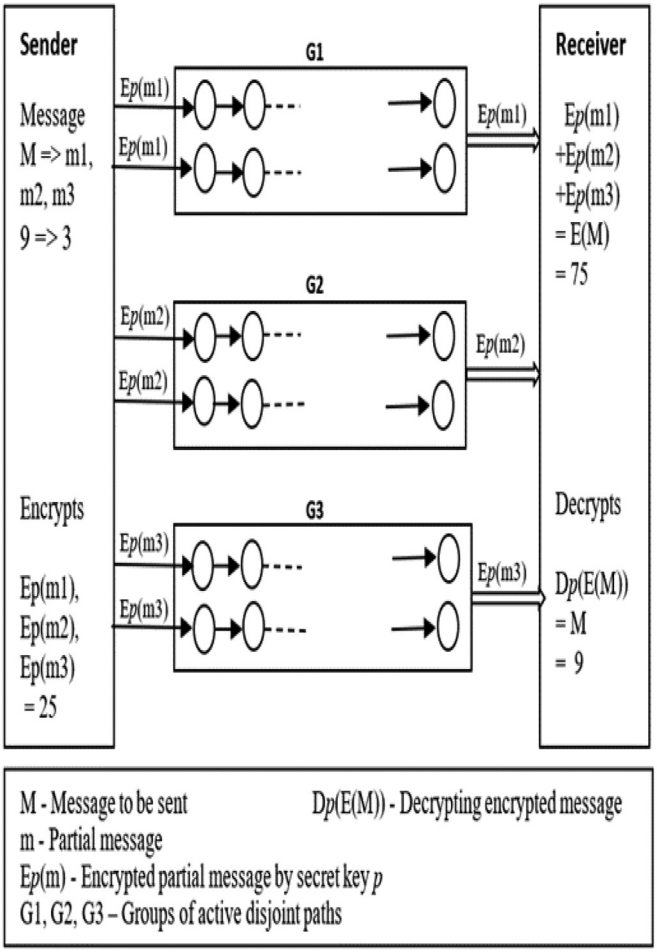

Fig. 3. An example of the proposed scheme where $n = 6$ and $G = 3$.

adding message part ids ($msg - sp - id1 + msg - sp - id2 + msg - sp - id3$) using the additive property in homomorphic encryption scheme to reach the sum of message parts *msg-sp-id-sum* = 6. When the received part is duplicated with already received message part ID, then the receiver discards it.

$$E\ (m1) + E\ (m2) + E\ (m3) = 25 + 25 + 25 = 75 = Y$$

- Decrypt the sum of the encrypted parts of entire message to get the original message at the receiver using EHC.

Decryption process:

$Y = E\ (m1) + E\ (m2) + E\ (m3) = 75$ and shared key
$p = 11\ Dp\ (Y) = Y\ mod\ p$
$= 75\ mod\ 11 = 9 = M$ (The original message)

In this scheme, the receiver can recover the whole message even though the data are dropped through $(n/G) - 1$ disjoint paths due to blackhole attacks because data is received via another safe path available in the group. Also, the entire message cannot be revealed to an attacker even if the node is compromised because the attacker gets only a part of the encrypted message, not the entire message. Hence, original data is recovered successfully.

5.3. Proposed scheme

Proposed algorithm – the sender procedure

Input: message *M*, number of active disjoint paths *n*
Output: Encrypted part of message E(*m*)

1: Read *M, n*	// read the entire message and number of active paths between source and destination.
2: Set *r*	// number of required disjoint active paths in each group.
3: Set *G* to *n* / *r*	// *G* is the number of groups of disjoint paths.
4: Set $m = M / G$	// splitting the original message.
5: Set *msg-id* to *1*	// assign 'message id' value for the whole message.
6: msg-sp-id-sum = 0	// initiate value of the sum of message parts.
7: ***for*** ($i = 1$; $i \leq G$; i++)	
8: Set *msg-sp-id* to *i*	// assign 'id' to part of the message.
9: Set *E(m)* to encrypt *m*	// encrypt part of the message.
10: *msg-sp-id-sum* + = *msg-sp-id*	// add to get the sum of message split ids.
11: Write *msg-id, msg-sp-id, E(m)*	// buffer output data.
12: ***end for***	
13: Write *msg-sp-id-sum*	// attend sum of message split ids to the buffer of output.
14: Send *msg-id, msg-sp-id, msg-sp-id-sum,E(m)*	//send output data to destination.

Proposed algorithm – the receiver procedure

Input: msg-id, msg-sp-ids, msg-sp-id-sum, encrypted message *E(m)*
Output: the original message *M*

1: Set *sum* = 0, *E*(*M*) = 0	
2: ***While*** (sum != *msg-sp-id-sum*) ***do***	
3: ***if*** (*msg-sp-id* is duplicated) ***then***	// msg-sp-id of encrypted message is already received.
4: drop *E(m)*	// drop the duplicate encrypted message.
5: ***else***	
6: add *E(M)=E(M)+E(m)*	// add encrypted parts of message.
7: sum = sum+ *msg-sp-id*	// add message split ids of the encrypted parts.
8: ***end while***	
9: *M* = decrypt E(*M*)	// decrypt sum of the encrypted parts to get the original Message.

Now, we analyze time complexity of our proposed scheme. In EHC, key generation, encryption, and decryption run in time polynomial (λ) where λ is a security parameter specifying the bit-length of the keys. To simply the analysis, let us assume that one encryption time in EHC is *T*. Since decryption time in EHC is much smaller than encryption time, the encryption time dominates, and *T* is the execution time in EHC. The overhead of using EHC in our proposed scheme is $T \times \theta(G)$. Note that *G* is the number of groups of disjoint paths, and *n* is the number of active disjoint paths between a sender and a receiver.

Next, we analyze the time complexity of the sender's procedure in our proposed scheme. The initialization steps (1 to 5) take $\theta(1)$, respectively. Encryption steps (6 to 12) repeat *G* times, so it takes $T \times \theta(G)$ times. So, the computational time complexity of the sender's procedure is $T \times \theta(G)$. The communicational time complexity in 14 is $\theta(G)$ since the sender transmits E(m) and msg-sp-id *G* times. The storage for *msg-sp-id* and E(*m*) needs $\theta(G)$ times, and the storage for *msg-id* and *msg-sp-id-sum* takes $\theta(1)$ time. The storage for *n* paths is $\theta(n)$ times. Now, we analyze the time complexity of the receiver's procedure in our proposed scheme. The initialization step (1) takes $\theta(1)$. The addition steps (2 to 8) take $\theta(G)$ times. The decryption time (9) takes $O(T)$ times. So, the computational time in the receiver's side is smaller than that in the sender's side. The storage requirement in the receiver's side is also smaller than that in the sender's side. Therefore, the time com-

Table 1
Comparison of time complexity between our proposed scheme and the original AOMDV scheme.

Scheme	Memory	Encryption	Decryption	Computation	Communication
our proposed	$\theta(n) + \theta(G)$	$T \times \theta(G)$	$T \times \theta(1)$	$T \times \theta(G)$	$\theta(n)$
AOMDV	$\theta(n)$	–	–	$\theta(1)$	$O(n)$

plexity in the sender's side is the time complexity in our proposed scheme.

In the original AOMDV scheme, the storage requirement for n paths is $\theta(n)$. Neither encryption nor decryption is used. So, the computational complexity is $O(n)$. The communicational time complexity is also $O(n)$ in the worst case. Table 1 summarizes the comparison of time complexity between our proposed scheme and the original AOMDV scheme.

6. Analytical model

In this section, we analyze our proposed algorithm through numerical modeling. When we assume that a source node has n disjoint routes to the destination, we can model each route as a queue Qi, which has a service rate μi and arrival rate λ from the source node as shown in Fig. 4. Since a route consists of number of nodes, the buffer capacity of each route is the sum of buffers in all nodes. Hence, we use the $M/M/1$ queue under the assumption that each queue has an infinite buffer for traffic and the service discipline is FCFS. Fig. 4 shows the queue model used in our analysis.

6.1. M/M/1 queue

To analyze the $M/M/1$ with Poisson arrivals (exponential inter-arrival times) and exponential service times, we need to know only the mean arrival rate λ and the mean service rate μ. Quantity λ/μ is called the utilization factor (traffic intensity) of the server and is denoted by ρ. The stability condition of the queue is $\rho < 1$. Below is a list of properties of $M/M/1$ queue.

Definition 1 Mean waiting time:

$$E[w] = \rho \frac{1/\mu}{1 - \rho} \tag{1}$$

Definition 2 Mean response time:

$$E[r] = (1/\mu)/(1 - \rho) \tag{2}$$

From this model, the total expected waiting time W_i in Q_i just for one packet is the mean response time.

$$W_i = (1/\mu)/(1 - \rho) \tag{3}$$

Let α_i be the throughput that can be expected in Q_i.

$$\alpha_i = \frac{parts\ of\ the\ data}{W_i} \tag{4}$$

Now, we can obtain β the throughput of the proposed protocol during W_i as follows:

$$\beta = \sum_{i=1}^{n} \alpha_i \tag{5}$$

where n is the number of active disjoint paths.

Each route as a queue has a service rate μ equal to 2 packets/second and arrival rate λ equal to 1 packet/second. We assume that we have four different scenarios for our MANET topology such as no malicious node (no packet loss), one malicious node into the active route, two malicious nodes into two active routes and also, three malicious nodes in the topology, respectively. Table 2 lists the results of the total throughput obtained from the analytical results with those obtained from the simulation results.

6.2. Our example scenario

$\lambda = 1$ packet/second, $\mu = 2$ packets/second and packet size = 512 bytes. Waiting time W_1 in Q_1 just for one packet is the mean response time .

$$W_i = (1/\mu)/(1 - \rho) = (1/2) \ / \ (1 - 0.5) = 1\ sec$$

From our proposal, dividing the first packet for sending it into $M/M/1$ queues and the capacity of each queue is one packet per second, so the source sends three packets to utilize the whole size of the queue.

$$4,096\ bits \ / \ 3\ (\#\ of\ groups) = 1,365\ bits$$

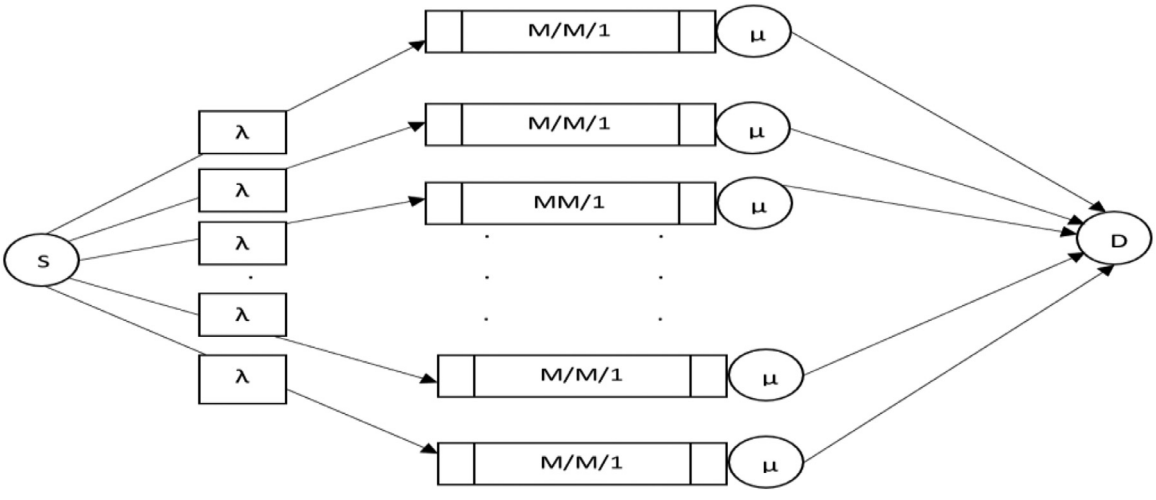

Fig. 4. Queue model for the proposed protocol.

Table 2
Comparing the throughput obtained from the analytical results with those obtained from the simulation results.

Number of malicious nodes	Numerical results (kbps)	Simulation results (kbps)
0	24.57	72
1	20.47	57
2	16.38	59
3	12.28	39
4	8.19	34
5	4.06	24

Table 3
Simulation parameters.

Simulator	Network simulator 2.35
Number of nodes	100
Malicious nodes	0, 1, 2, 3, 4, 5
Area	1100 m × 1100 m
Communication range	250 m
Packet size	512 bytes
Interface type	Phy/Wireless phy
MAC type	IEEE 802.11
Queue length	50 packets
Propagation type	TwoRayGround
Routing protocol	AOMDV
Transport agent	UDP
Application agent	CBR
Traffic rate	1 kbps
Simulation time	900 s

The throughput that can be expected in a single queue such as Q_1 is:

$$\alpha_1 = \frac{parts\ of\ the\ data}{W_1} = 4096\ bits/sec$$

The total throughput β of all queues $Q's$ during $W_i's$ is :

$$\beta = \sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{6} \alpha_i$$
$$= \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 + \alpha_6 = 24,\ 576\ \text{bits/sec}$$

In this case, n is the number of active disjoint paths between the source and the destination, and there is no malicious node within any of these active paths. But in the case of malicious node's presence, the throughput for a single queue is zero due to the dropping of data by the malicious node.

7. Performance evaluation

In this section, the simulation results for performance evaluation are presented. First, the simulation methodology and performance matrices are explained and then the simulation results are given.

7.1. Performance methodology and performance metrics

We make a simulation using network simulator (NS-2) [23]. The AOMDV protocol is modified to simulate our proposed scheme with several malicious nodes. We define 100 nodes for our simulation. Some of those nodes are simulated as blackhole nodes. Each node in a MANET is assigned an initial position within the simulation dimensions (1100 × 1100 m). The packets are generated using CBR with packet size 512 bytes for all mobile nodes. 10 m per second is used as the mobility of each node. The simulation lasted 900 s. We use IEEE 802.11 MAC protocol. Table 3 lists the simulation parameters.

To evaluate the performance, we simulated the original AOMDV protocol and our proposed scheme in the following four metrics as a function of number of attackers:

- Packet delivery ratio (%): the proportion of the total number of packets reached the destination over the number of packets sent by the source.
- Throughput (bits/sec): the amount of data successfully received at the destination per second.
- Packet loss (%): the average number of lost packets during the data transmission process.
- Average end-to-end delay (sec): the time taken for a packet to reach the destination from the source node.

Also, we consider node mobility scenarios to analyze the simulation results based on the performance metrics as below:

- Packet delivery ratio (%).
- Throughput (bits/sec).

7.2. Simulation results

7.2.1. Packet delivery ratio

Refer to Fig. 5. Here, the packet delivery ratio (PDR) is compared between our proposed scheme and the original AOMDV protocol as a function of malicious nodes (blackhole attackers). When one attacker is launched into one of the active routes, PDR is decreased in the original AOMDV scheme but there is no big impact in AOMDV when the number of attackers is increased more than one for a single data transmission flow through the same active route because the AOMDV scheme utilizes only a single path at a time. Hence, the first attacker involved in the single path only will create a big impact and the rest of the attackers will not create any significant impact since the original data is already dropped. In the meantime, our proposed scheme maintains the PDR because the original data is received somehow by using any one of the paths from the number of paths in the group. Hence, the original data is recovered properly. Here, we observe that in the presence of any malicious nodes, the packet delivery ratio reduces too much in the original AOMDV, but it stays holding close in our proposed scheme,

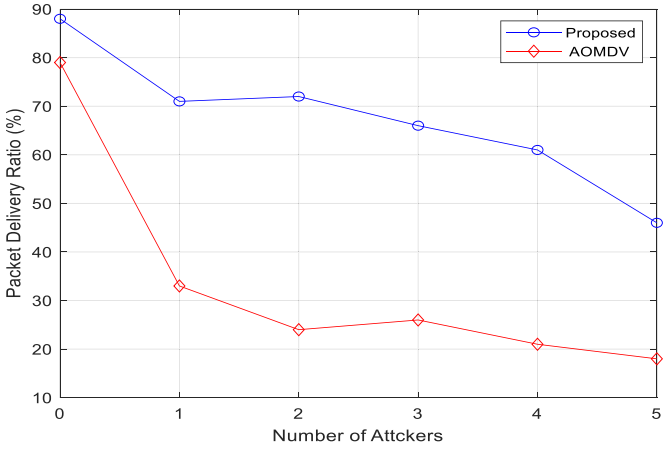

Fig. 5. Impact of packet delivery ratio as a function of malicious nodes.

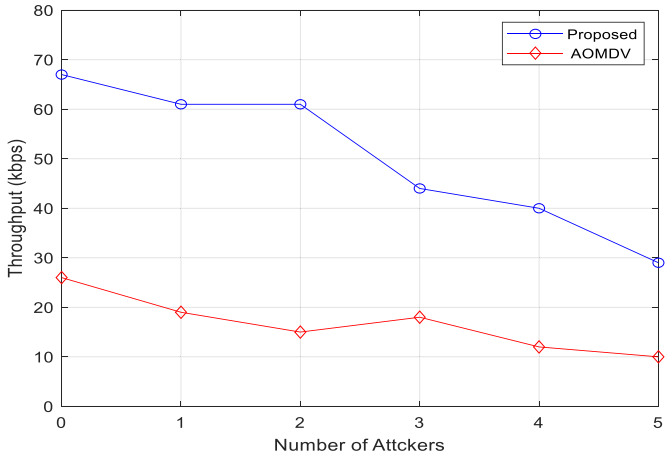

Fig. 6. Impact of throughput as a function of malicious nodes.

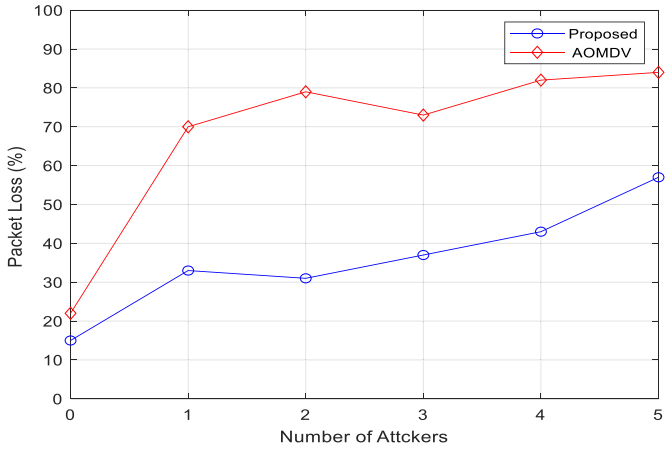

Fig. 7. Impact of packet loss as a function of malicious nodes.

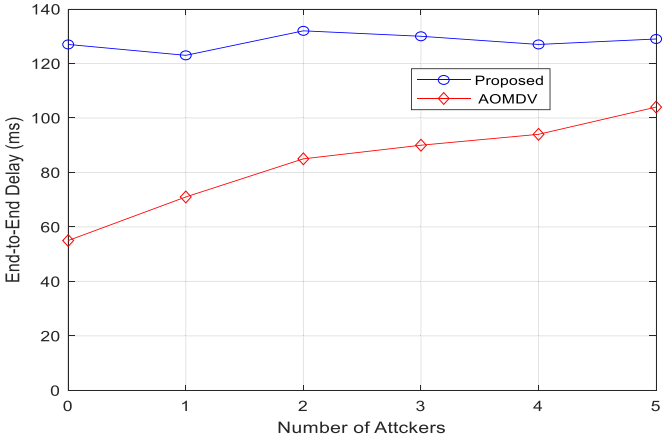

Fig. 8. Impact of end-to-end delay as a function of malicious nodes.

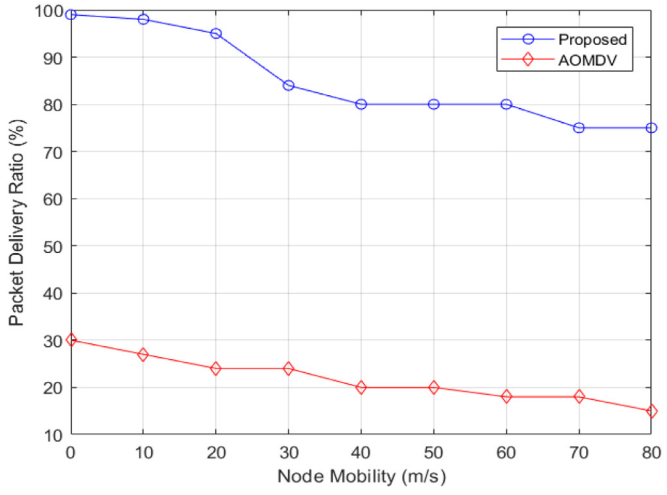

Fig. 9. Impact of packets delivery ratio as a function of node mobility.

and more malicious nodes give less packet delivery. As seen, our proposed method has shown a good performance in packet delivery compared to the original method.

7.2.2. Throughput

In Fig. 6 we compare the throughput of schemes as a function of malicious nodes (blackhole attackers). When an active attacker is present in the network, the amount of data successfully received at the destination per second is decreased in both schemes because of the long duration of data transmission. But our proposed scheme still provides higher throughput than the original AOMDV scheme due to the high PDR when the number of attackers is increased. Even though our proposed scheme takes more time for delivering the packet, it is more reliable to deliver the packet when malicious nodes are increased. Here, we observe that throughput is higher in our proposed scheme compared to the original scheme for the packet transmission.

7.2.3. Packet loss

The packet loss of the schemes is compared in Fig. 7 as a function of blackhole attackers. In general, when the number of active attackers is increased within multipath routing protocols, packet loss is increased. In the original AOMDV protocol, there is slight impact on the packet loss when the attacker is increased more than one for a single data transmission because the scheme utilizes only a single path at a time. Thus, the first attacker involved in the single path only will create a big impact and the rest of the attackers in the same active route will not create any significant impact because the encrypted message has already dropped by the first attack. But there is an impact of multiple attackers in the proposed protocol because the scheme utilizes multiple paths simultaneously. Even though the impact is present with higher data loss in our proposed scheme by increasing the malicious modes, it delivers almost whole packet to the destination by distributing it into multiple paths to ensure the entire delivery through safe paths.

7.2.4. End-to-End delay

In Fig. 8 we compare the end-to-end delay of both schemes as a function of blackhole attackers. The delay is higher in our proposed scheme than the original AOMDV scheme when the number of malicious nodes is increased due to its procedures and security features. According to the data packet delivery ratio when the number of malicious nodes is increased, our proposed scheme can deliver data better than other methods, but it must divide and encrypt the message to achieve this feature. Due to this reason, it takes more delay for the delivery.

7.2.5. The impact of mobility on performance

Fig. 9 depicts the effect of the packet delivery ratio on the node mobility in the presence of the blackhole attack in the network, where node mobility (meter per second m/s) is the rate at which the nodes are moving in the network. We observe that AOMDV suffers heavy loss in packets in the presence of a blackhole node, by dropping from above 30% to below 20%. However, our protocol

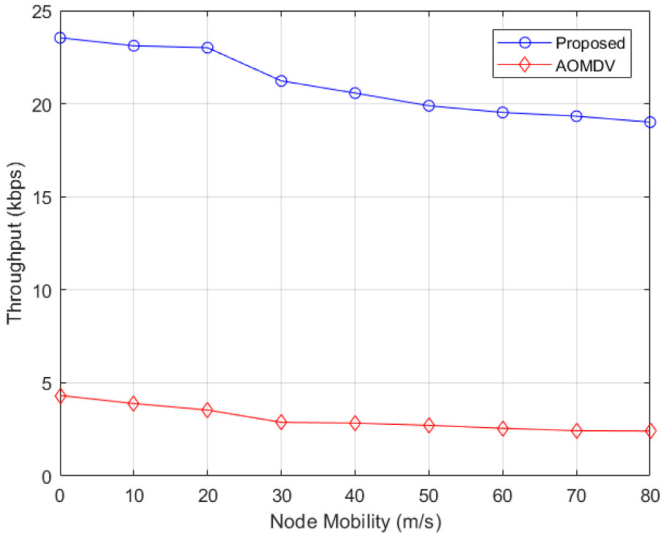

Fig. 10. Impact of throughput as a function of node mobility.

scheme gives a higher packet delivery ratio, not less than 75% in the node mobility 80 m/s even in the presence of a blackhole node.

Also, the effect of the network throughput on the node mobility is depicted in Fig. 10. We observe that the standard AOMDV protocol under blackhole attack has much lower throughput when compared to that of our proposed scheme. Moreover, when an active attacker is present and the node mobility is increased in the network, the amount of data successfully received at the destination per second is decreased in both schemes but still our proposed scheme holds very high throughput compared to the original protocol.

8. Conclusion

In this paper, we proposed an extended AOMDV scheme to make data transmission be reliable and secure in the presence of malicious nodes in MANETs by distributing the parts of entire message into multiple paths and using a homomorphic encryption method for cryptography. The simulation results show that the proposed scheme provides a higher packet delivery ratio and throughput, which are good features for the emergency applications in MANETs. Moreover, the success rate of the proposed scheme to ensure and guarantee the delivery of the packet to the target is very high with many active paths in each group of the network.

Further research will be done in decreasing end-to-end delay to apply this scheme to the emergency applications in MANETs.

Comment: Earlier version of this paper was presented to IEEE CCWC (The 8th IEEE Annual Computing and Communication Workshop and Conference), Las Vegas, NV, USA, Jan. 2018.

Declaration of Competing Interest

None.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.jisa.2019.102425.

References

[1] Das M Marina S. On-demand multipath distance vector routing in ad hoc networks. Ninth international conference on network protocols ICNP Riverside, CA, USA. IEEE; 2001.
[2] Zheng Y, Zhao Z, Zhu J. Improved AOMDV with precaution algorithm in wireless ad hoc networking. In: IEEE International conference on control and automation. IEEE; 2009. p. 175–9.
[3] Parmar PV, Padhar SB, Patel SN, Bhatt NI, Jhaveri RH. Survey of various homomorphic encryption algorithms and schemes. Int J Comput Appl 2014;91:26–32. doi:10.5120/15902-5081.
[4] Chlamtac I, Conti M, Liu JJN. Mobile ad hoc networking: imperatives and challenges. Ad Hoc Netw 2003;1:13–64. doi:10.1016/S1570-8705(03)00013-1.
[5] Papadimitratos P, Haas ZJ. Secure message transmission in mobile ad hoc networks. Ad Hoc Netw 2003;1:193–209. doi:10.1016/S1570-8705(03)00018-0.
[6] Lou W, Liu W, Fang Y. SPREAD: enhancing data confidentiality in mobile ad hoc networks. Proc IEEE INFOCOM 2004;4:2404–13. doi:10.1109/INFCOM.2004.1354662.
[7] Wazid M, Kumar A. A secure group-based blackhole node detection scheme for hierarchical wireless sensor networks. Wirel Pers Commun 2017;94:1165–91. doi:10.1007/s11277-016-3676-z.
[8] Wazid M, Kumar A. An efficient hybrid anomaly detection scheme using K-means clustering for wireless sensor networks. Wirel Pers Commun 2016;90:1971–2000. doi:10.1007/s11277-016-3433-3.
[9] Wazid M, Das AK, Kumari S, Khan MK. Design of sinkhole node detection mechanism for. Secur Commun Netw 2016;9:4596–614. doi:10.1002/sec.
[10] Satav P, Jawandhiya P, Thakare V. Secure route selection mechanism in the presence of black hole attack with aomdv routing algorithm. 2018 Fourth international conference on computing communication control and automation. IEEE; 2018.
[11] Yang H, Shu J, Meng X, SCAN SLu. Self-Organized network-layer security in mobile ad hoc networks. IEEE J Sel Areas Commun 2006;24:261–73.
[12] Chelvan KC, Sangeetha T, Prabakaran V, Saravanan D. EAACK-A secure intrusion detection system for. Int J Innov Res Comput Commun Eng 2014;1:3860–6.
[13] Tan S. Using cryptographic technique for securing route discovery and data transmission from blackhole attack on AODV-based MANET. Int J Netw Distrib Comput 2014:100–7. doi:10.2991/ijndc.2014.2.2.4.
[14] Ertaul L, Chavan N. Elliptic curve cryptography based threshold cryptography (ecc-tc) implementation for manets. IJCSNS Int J Comput Sci Netw Secur 2007;7:48–61. http://paper.ijcsns.org/07_book/200704/20070407.pdf.
[15] Sultana J, Ahmed T. Securing AOMDV protocol in mobile adhoc network with elliptic curve cryptography. 2017 International conference on electrical, computer and communication engineering. IEEE; 2017. doi:10.1109/ECACE.2017.7912964.
[16] Jain G, Rajawat G. Secure AODV routing protocal based on homorphic digital signature. 2nd International conference on contemporary computing and informatics; 2016. doi:10.1109/IC3I.2016.7917980.
[17] Rangasami K, Vagdevi S. Comparative study of homomorphic encryption methods for secured data operations in cloud computing. International conference on electrical, electronics, communication, computer, and optimization techniques; 2017.
[18] Ahmed G, Barskar R, Barskar N. An improved DSDV routing protocol for wireless ad hoc networks. Procedia Technol 2012;6:822–31. doi:10.1016/j.protcy.2012.10.100.
[19] Liu S, Yang Y, Wang W. Research of AODV routing protocol for ad hoc networks1. AASRI Procedia 2013;5:21–31. doi:10.1016/j.aasri.2013.10.054.
[20] Chen Y, Xiang Z, Jian W, Jiang W. A cross-layer AOMDV routing protocol for V2V communication in urban VANET. In: Fifth international conference on mobile ad-hoc and sensor networks; 2009. p. 353–9. doi:10.1109/MSN.2009.30.
[21] Ertaul L, Vaidehi. Implementation of homomorphic encryption schemes for secure packet forwarding in mobile ad hoc networks (MANETs). IJCSNS Int J Comput Sci Netw Secur 2007:132–41.
[22] Ahirwal RR, Ahke M. Elliptic curve diffie-hellman key exchange algorithm for securing hypertext. Inf Wide Area Netw 2013;4:363–8.
[23] Teerawat Issariyakul EHE.H. Teerawat Issariyakul. Introduction to network simulator NS2. second. Springer Science+Business Media; 2012.