Optimize and Secure Routing Protocol for Multi-hop Wireless Network

Salwa Othmen[1], Wahida Mansouri[2], Somia Asklany[3], Wided Ben Daoud[4]
Computers and Information Technology Department, College of Science and Arts[1, 2, 3]
Turaif, Northern Border University, Kingdom of Saudi Arabia[1, 2, 3]
NTS'Com Research Unit, ENET'COM, University of Sfax, Sfax, Tunisia[4]

***Abstract*—Multi-hop Wireless Network (MWN) requires the existing of wireless nodes that communicate via a wireless channel. Thus, selecting optimal paths between the communicant nodes is a major challenge. Many researchers are focusing on this topic and proposed some routing protocols that help the nodes to learn multi-hop paths. Multi-hop wireless network is used for several types of applications, like military, medical care and national security. These applications are important and critical, so they require a certain level of performance and security during data communication. Securing the transmission of data in a multi-hop network is a challenge since the devices have limited resources like memory and battery. In this paper, we propose an optimal and secure routing protocol. The main goal of this proposal is to improve the performance and the security of such network by selecting a secure route between the source and its target destination. To secure data transmission phase, we propose to create a key shared between the source and the destination. Since the devices have limited energy, we propose to take into consideration the energy of the intermediate nodes of the selected route. Extensive simulations are performed using the Network Simulator (NS2) to validate the proposed protocol. This proposal is compared with the secured Ad-Hoc On-demand Distance Vector (SAODV) in terms of end-to-end delay, overhead and number of compromised devices.**

***Keywords*—Mutli-hop wireless network; routing protocol; Diffie-Hellman; Weil Pairing; NS2**

I. Introduction

Multi-hop Wireless Networks (MWNs) like Ad Hoc networks, sensor networks and Internet of things (IoT) compose of wireless and discrete devices that communicate with each other directly without needing any fixed infrastructure [1]. Thus, the main function of such network is to route the information from the source to the destination from a node to another. This is performed by exchanging route information across different devices of the network. Many researchers are interested in this important topic and try to propose routing protocols which allow the devices to learn some multi-hop route between them. The routing protocols are classified into three categories: reactive, proactive and hybrid protocols.

In the proactive protocol, each node maintains a routing table that contains information about existing routes. When a node tries to transmit data, it uses a route already exist in this routing table. Many proactive routing protocols are proposed like Optimized Link State routing protocol (OLSR) [2], Destination Sequence Distance Vector (DSDV) [3] and Wireless Routing Protocol (WRP) [4], etc. However, in the reactive protocol, only one active route is required to reduce the overhead in the network like Dynamic Source Routing (DSR) [5], Temporarily Ordered Routing Protocol (TORA) and Ad-Hoc On Demand Distance Vector (AODV) [6]. The hybrid protocol is a combination of the reactive and the proactive protocols.

Many challenges may affect the use of multi-hop wireless networks to support many applications due to their specific characteristics like the unstable topology, energy efficiency and mobility, etc. Therefore, it is important to take into account these challenges when designing and improving the functions of MWN such as the multi-hop routing protocols.

Another important issue must be taken into consideration when designing a routing protocol for MWN, is the security due to the participation of the nodes in the routing process. Indeed, an attacker can participate in the route discovery phase to become a member of the selected route and it can later perform different types of attacks like dropping, forging or injecting data packet. However, introducing security in multi-hop routing protocols needs extra resource consumption and extra storage due to the underlying computation cost required. This is not desirable in MWN as the limited resources of the nodes. Thus, when securing the routing in MWN, an efficient use of resources should be considered, in particular the energy resource.

However, many proposed protocols handle the resource efficiency and the security separately.

The security of routing protocols is mandatory to provide the protection of the exchanged data from the source node to the destination node. Most of the proposed protocols ensure the security from sharing secret keys between each two neighbor nodes. Thus, the number of the shared keys increases with the increase of the nodes in the network. This is lead to high resource consumption, which is not efficient, especially for some critical networks like the sensor networks due to the limited resources of the sensor nodes.

In this paper, we propose a new multi-hop routing protocol for MWN. This proposal selects secure and optimal path that ensures security in terms of authentication, confidentiality and integrity. For achieving the anonymity, we propose to use a temporary identity for each node in the communication process. The battery life of the selected nodes is taken into account in the proposal to achieve the performance of such

network. Indeed, during the route discovery process, only the nodes with high energy can be selected. When a destination receives several request packets, it selects the shortest and the longest lifetime route based on a proposed cost function.

The current paper is organized as follows: Section 2 offers an overview on some related works. Section 3 provides a detailed description of the proposed routing protocol. The last section makes the conclusion of the work and suggests the future research.

II. Related Work

Many routing protocols are proposed in the literature to optimize the performance of the MWNs. Indeed, in [7], a multi-hop routing protocol using cellular virtual grid in internet of thing environment is proposed. The goal of this proposal is to prolong the network lifetime through the balancing of energy consumption. The cost of the path between the source and the destination nodes is computed based on the residual energy and the distance. In [8], O. Salwa et al. proposed a fuzzy logic based on-demand routing protocol for multi-hop cellular networks. To optimize the performance of the network, the authors combine threes metrics which are Signal to Interference and Noise Ratio (SINR), residual energy and gain time, based on the fuzzy logic system. In [9], a low-overhead multi-hop routing protocol for device to device communication in 5G is proposed. The proposal is based on the DSR protocol to select an optimal route for 5G in a short time. The overhead is reduced through the minimizing of the exchanged control messages, so the time and the energy are saved during the route discovery process. These three protocols [7-9] improve the networks performance in terms of energy consumption and lifetime.

However, the main drawback of these proposals is that they do not take into account the security requirements.

Other works are proposed to secure and optimize the routing protocol for multi-hop networks. Indeed, in [10] H. Kojima et al. proposed to secure DSR protocol using sequential aggregate signature in order to sign the routing information. In this proposal, the communication between devices requires a centralized key generation center to distribute the keys in the network. Thus, any new device cannot join the network without authentication to this center. In [11], G. Singh et al. proposed a routing protocol called Expiration Time based Routing Protocol (LETSRP) which based on a one-time signature scheme to authenticate the exchanged data in the network. Before sending any packet, each node computes the time expiration of its links using a greedy algorithm. The number of the sent packets depends on the available bandwidth. In [12], a secured and optimized routing protocol for MANET is proposed by A. Bhusari et al. This work was designed to optimize the performance of the routing protocol by minimizing the overhead and the delay. To secure this proposed protocol, a new metric based on cross layer design is provided to defend several attacks. To secure the request phase, the source node signs the RREQ with the group signature based on its private key. The destination node decrypts the received packet using the public group signature key.

However, the disclosure of the generated signature may cause the disclosure of the entire network. This is because the nodes use the same key during the communication process.

In [13], A. Vinitha et al. proposed a secure multi-hop routing protocol for wireless sensor networks. To secure the proposed protocol, the authors employed a trust model using several trust factors like indirect trust, direct trust, forward rate factors and integrating factor. To ensure the optimization of the proposal, the trust factors are integrated with other parameters such as delay, distance, energy, intra-cluster distance and inter-cluster distance. Before selecting the optimal route, the network is devised into a several cluster. The cluster heads are selected based on the Low Energy Adaptive Clustering Hierarchy (LEACH) protocol.

In [14], K. Hamouid et al. proposed a secure tree-based routing protocol for wireless sensor networks. The authors use ID-Based authentication key-agreement protocol to secure the data routing between the nodes in the network. The confidentiality and the authenticity are provided in the proposed protocol with low cost. Indeed, each node in the network is preloaded with a private key used to generate shared keys with its neighbor nodes. Moreover, to reduce the communication overheads a single message is transmitted by each node for both key –establishment and routing-tree construction. However, in this protocol, each node must perform complex operations to generate security keys. This may increase the energy consumption by the nodes.

In [15], Zapata et al. proposed a secure routing protocol called Secure Ad Hoc On-Demand Distance Vector (SAODV) which is an extension of the AODV protocol to guarantee its security in terms of authentication, integrity and non-repudiation. To achieve the authentication, the source and the destination nodes add their signatures based on their private keys. The intermediate nodes only check the validity of this generated signature without any authentication performed between each other. However, to achieve the integrity of the hop-count field, a hash chain is used. The function used to compute the hash value is added to the hash function field. The SAODV protocol uses several mechanisms to secure the route request phase, but it remains vulnerable to many types of attacks. This fact is due to the lack of the authentication between neighbor nodes. Indeed, an adversary can participate in the selected path without modifying the hop-count field by using the same hash value. Thus, the legitimate nodes cannot detect this attack. In [16], M. Surajuddin et al. proposed a routing protocol that takes into account multiple factors such as packet loss reduction, congestion, malicious node detection and security of data transmission. Indeed, the source broadcasts a RREQ packet, which contains a fake destination address and sequence number. Only an attacker will respond with a RREP packet. In this case, the source maintains the address of this attacker in a black list and propagates this information to the other nodes in the network. Moreover, each node has a trust value calculated based on the opinion of its neighbors. Through this trust value, the nodes can identify the malicious nodes which have a trust value less than a threshold. However, this proposed protocol is not secured against several types of attacks like the impersonation attack and Sybil attack.

To overcome some limitations of the existing works like the lack of authentication between the neighbor nodes and the complex operations to compute a shared key, etc., we propose a new protocol described in the following section.

III. Proposed Protocol

A. Weil Pairing

In the proposed protocol, we are based on Weil Pairing tool for key generation. Indeed, the Weil Pairing [17] is an important method used in elliptic curve systems, key generation and identity-based encryption.

Let two groups G1 and G2 of order q, note that G1 is an additive cyclic group over an elliptic curve and G2 is a multiplicative cyclic group. P is a generator of G1. The admissible bilinear map:

ê: G1 ×G1⟶G2 has the following properties:

- Bilinear: for all P, Q ∈ G1 and for a, b ∈ Z, ê(aP, bQ) = ê(P, Q)^{ab}.
- Non-degenerate: if P, Q ∈ G1 such that ê (P,Q) ≠ 1.
- Computable: for all P, Q ∈ G1, ê (P,Q) can be computed efficiently.

B. Network Model

In the proposal, we consider a MWN which consists of multiple devices distributed randomly in a geographical area and a trusted party (TP). Each device has a unique identity in the network (ID). We assume that these devices are not secured and so they can be compromised, but we suppose that TP is secure and trustworthy. Thus, we suppose that the TP is responsible for the generation and the record of the system parameters in a secure way.

These parameters are as follows:

- p is a large prime number,
- G1 and G2 are two cyclic groups.
- g is a generator in Z^*_p,
- P is a generator of G1,
- H: is a hash function, {0, 1}* →G1,

The TP generates a private key called s ∈ Z^*_q , and a master key P_{pub} = sP. Then, it bootstraps the devices with initial secret parameters in offline before network deployment. Indeed, it assigns a private key for each device; $S_i = sQ_i$, where $Q_i = H(ID_i \| t)$, t is the timestamp initiated by the TP in order to prevent the network against replay attack. Before the route discovery process, each device D_i must compute and share a secret key with the devices located at n hops. For that reason, it generates a random value called R_i and sends to the neighbor devices the following value: $P_i = R_iP$ used to compute the shared key. This value is based on Pairing Discrete Logarithm Problem (PDLP) which is a complex problem because finding the integer R_i is hard.

C. Description of the Proposed Algorithm

The proposed routing protocol is divided into three phases: route request, route reply and data transmission phases. This protocol is proposed for MWN which is a hostile environment where it can be intercepted by different types of attacks. Thus, a high level of security must be achieved to secure each phase among the phases listed below. In addition to security challenge, the MWN face other major challenges like energy constraint of devices. Indeed, energy is a critical resource in MWN as its lifetime depends on battery depletion of mobile devices. More energy consumed in the routing process leads to reduce the network lifetime. For that reason, in the proposed routing protocol, we ensure an efficient use of the limited resources, in particular the energy consumption.

1) Route request phase: When a source device (S) intends to communicate to a destination device (D) and it does not have a valid route, it initiates the route request phase by broadcasting a route request (RREQ) packet to all its neighbors. It is based on Location based-Multiple metric (LoMM) to reduce the number of the devices that can receive the RREQ packet. This is to exclude the devices that are further away from D to participate in routing data. By this way, the end-to-end delay and the signaling load are reduced. Moreover, this metric reduce the complexity of the computational operations as all devices are participating in computing a group key and so reducing the energy consumption in the network.

To secure the request phase, each two neighbor devices share a secret key. During this step, the two devices perform a mutual authentication between each other at the same time. To reduce the computational complexity, the neighbors perform just a single evaluation of the Weil Pairing as compared with other schemes like Smart-Chen-Kudla scheme.

The generation of the shared key K_{ij} between each two neighbor devices D_i and D_j is performed as follows:

D_i computes K_{ij} using the following equation (1):

$$K_{ij} = \hat{e}(S_i;\ R_jQ_j + R_iQ_j)$$

$$= \hat{e}(sQ_i;\ R_jQ_j + R_iQ_j)$$

$$= \hat{e}(Q_i; Q_j)^{s(Ri+Rj)}$$

In the other side D_j computes also K_{ji} as the following function:

$$K_{ji} = \hat{e}(R_iQ_i + R_jQ_j;\ R_j)$$

$$= \hat{e}(R_iQ_i + R_jQ_j;\ sQ_j)$$

$$= \hat{e}(Q_i; Q_j)^{s(Ri+Rj)}$$

$$= K_{ij}$$

Where, R_i and R_j are random values generated by D_i and D_j respectively, and exchanged based on Pairing Discrete Logarithm Problem as mentioned above.

The source initiates the route request phase by broadcasting a RREQ packet to all its neighbors. The format of the RREQ is as follows:

RREQ:{ID_S, E(K_{sj},ID_D||seqNb||TTL||Hop-count||K_{PK_S}(g^{Rs}modp) || ME) ||MAC_{Ksj}(ID_S, ID_D , seqNb, TTL, Hop-count, K_{PK_S} (g^{Rs}mod p), ME)}

Where,

- K_{si} is the shared key between S and each of its neighbor D_j. It is calculated as the function (1) in order to encrypt the RREQ packet between each other and so to provide the confidentiality of this packet.
- ID_S is the source address,
- ID_D is the destination address,
- seqNb is the sequence number which prevents the RREQ packet against replay attack,
- TTL: is the Time To Live which limits the propagation area of the RREQ packet,
- Hop_count: is a value incremented by each intermediate node to count the number of hops in the discovered route,
- g^{Rs}mod p: is a value used to compute a shared key between S and D, where R_S is a random number generated by S. For more security, this value is encrypted by the private key of the source. Finding R_S is hard as it is difficult to resolve the Diffie-Hellman problem in prime order.
- ME: is the minimum remaining energy which represents the lifetime of the discovered route.
- MAC_{Ksj}: is a function used to check the integrity of the RREQ packet.

When an intermediate device D_i receives a RREQ packet from a neighbor D_j, it performs the following steps:

- Decrypts the received packet using the shared key K_{ij} with the sender device, which is calculated as the function (1). If this decryption is performed successfully, so that a mutual authentication is provided between them because only these two devices can calculate this shared key.
- Computes the MAC function to verify the integrity of the received packet. If there is no problem with the integrity, D_i passes to the next step, otherwise, it discards the received packet.
- Checks if it is the target destination by comparing its own address and ID_D. If it is the target destination, it sends back a response to the source via the reverse route if not, it performs the next steps,
- Checks if TTL is zero, it discards the received packet, if not it decrements this field and increments hop_count field,
- Computes its residual energy and compares it with the ME field, then it reassigns the ME field with the minimum value among them.
- Maintains the address of the sender in its routing table, and adds its address in the RREQ packet.
- Computes the MAC function using the key shared with each neighbor,
- Sends the RREQ packet to the neighbors after encrypting it by the secret key shared with each of these neighbors.

The RREQ packet is sent until it reaches the destination in a secure way.

D. Route Reply Phase

When the destination receives a RREQ packet, it waits for a definite time to receive other RREQ packets. Then it performs the following steps:

- It decrypts the received packets and checks their integrity. Then, it calculates the cost (C) of each discovered path as the following equation:

$$C = \frac{ME}{hop\_count}$$

- It selects the path with the largest cost C. By this way, it chooses the path that has the greatest remaining energy and the smallest number of intermediate nodes (shortest path).
- Computes the shared key with the source based on Diffie_Hellman problem as the following equation:

$$K_{DS} = g^{R_S * R_D} modp$$

Where, R_D is a random value generated by the destination. R_D is sent to the source using Diffie_Hellman problem $g^{R_D} modp$ to recalculate the shared key with the source as follows:

$$K_{SD} = g^{R_D * R_S} modp$$

Thus, the same key is obtained by the source and the destination:

$$K_{SD} = K_{DS}$$

- Generates the RREP packet:

RREP: {ID_D, E(K_{Dj}, ID_S|| ID_D ||K_{PK_D}($g^{R_D} modp$) || $MAC_{K_{Dj}}$(ID_S, ID_D , K_{PK_D} ($g^{R_D} modp$))}

The RREP is encrypted by K_{Dj} which is the shared key between the destination and the intermediate device j of the selected route. K_{Dj} ensure also a mutual authentication between the two communicants.

$MAC_{K_{Dj}}$ is used to check the integrity of the packet.

$g^{R_D} modp$ is encrypted by the private key of the destination for more security.

The RREP is sent through the reverse route until it reaches the source device.

When the source receives the RREP packet, it re-computes the shared key with the destination and triggers the transmission data phase secured by the shared key between the source and the destination.

IV. Security Analysis

In the following section, we analyze the security of the proposal against several threats by showing that it achieves the security constraints:

A. Confidentiality

The messages exchanged in the request and reply phases of the proposed protocol are encrypted with the keys shared between the neighbor devices. To compromise these keys, the attackers need to know the secret parameters used to calculate each key, and so they have to resolve the PDLP which is a hard problem.

Furthermore, the data transmission phase is secured based on the shared key between the source and the destination. To compromise this key, the attacker needs to resolve the Diffie-Hellman problem.

Thus, the proposed protocol ensures the confidentiality of the exchanged messages.

B. Authentication

In the proposed protocol, each two neighbors have to share a secret key based on Weil Pairing scheme. This method provides an implicit mutual authentication between the communicants using some secret parameters. Indeed, every device computes and shares a secret key with its neighbor; only a legitimate device can compute this key as it is based on the private key of the TP. Moreover, the source and destination authenticates each other through the shared key between them, which is calculated based on Diffie-Hellman problem.

Thus, the proposed protocol achieves the authentication.

C. Integrity

In the proposal, to check the integrity of each transmitted message, the sender adds the MAC function to this message. To forge the integrity of such packet, an attacker must decrypt it and re-compute the MAC function of the modified packet. However, this is not possible as the attacker does not learn the secret key used to encrypt the received packet.

D. Sybil Attack

Sybil attack occurs when an attacker use unauthorized identities to perform neighbor relationships with other legitimates devices. In the proposal, when an attacker sends messages to a legitimate device using a forged identity, it fails in performing a mutual authentication as it has not a valid key issued by the TP. Thus, to perform a Sybil attack, the attacker must generate its own private key, which is impossible because it is hard to solve PDLP problem and hold the private key of the trust party. For that reason, the proposal is secured against Sybil attack.

E. Replay Attack

The attacker tries to falsify the destination by retransmitting many authorized packets. The proposed protocol is secured against this type of attack for many reasons. First, because the source generates a sequence number for each new request packet. Second, the private key of each device is computed based on a timestamp initiated by the source. Moreover, the shared keys are based on a random number generated by legitimates devices in each session without any links with the values generated in the previous session. Thus, the proposed protocol is secured against replay attack.

F. Impersonation Attack

In this type of attack, the attacker uses a legitimate identity to perform a neighbor relationship or to participate in the selected route as an intermediate device. In this proposal, to impersonate a device, the attacker must compute a shared key with this device. However, it cannot obtain the same key computed by the legitimate device as it does not hold a private key assigned by the TP. Then, it is not feasible to resolve the PDLP and discover the private key of TP. Thus, it is not possible to impersonate a legitimate device.

V. Simulation Result

To evaluate the performance of the proposed routing protocol, we conduct extensive simulations using the network simulator (NS-2). We add to this simulator the security library Crypto++ as it supports many tools of security mechanism. The network is composed of 60 devices that move by Two Ray Ground model in 1000m*1000m area.

The parameters of the simulation are summarized as the following Table I.

The compromise of the legitimate devices is a major challenge which is hard to defend. If a device is compromised, the attacker can participate in the selected route and access to the exchanged messages and security parameters. Thus, all the devices can be affected. To evaluate the robustness of the proposed protocol against the malicious nodes, we introduce several attackers that held black hole attack. They pretend to be the target destination by sending RREP packets while it receives a RREQ packet, or they try to become members of the selected route.

TABLE I. Simulation Parameters

Parameters	**Value**
Routing protocols	Proposed protocol, SAODV
Simulation time	200 seconds
Simulation area	1000*1000
Traffic type	Constant Bit Rate (CBR)
Packet size	512 bytes
Queue length	250 packets
MAC protocol	MAC/802.11
Mobility model	Two Ray ground
Initial energy	150J
Transmission energy	0.5 W

The proposed protocol is compared with the SAODV protocol, then, we measure three metrics as follows:

1) End-to-end delay: is the average delay between the time of packet generation and the time of its reception by the receiver.

2) Overhead: is the average of the amount received messages by each device during the route establishment phase.

3) Number of compromised devices: is the total number of devices compromised by the attackers during simulation time.

Fig. 1 represents the results of the end-to-end delay as a function of the number of attackers. As we can see, the proposed protocol has less value of end-to-end delay than SAODV protocol. This is due to the fact that, the proposal selects the shortest secured path. Moreover, in the proposal, the risk that an attacker compromises a device and participates in the selected route is less than SAODV protocol. Indeed, if an attacker becomes a member of the selected route, it maintains the received packets more time to handle its content and extracts the needed information from these packets. Therefore, the delay required for a packet to reach the destination is increased.

Fig. 2 presents the results of the overhead versus the number of attackers. As we can see, in the proposed protocol the message load is reduced compared with the SAODV protocol when the number of attackers increases. This is because; in the proposal when a device receives a packet from an attacker it drops this packet, but with SAODV the devices resent every received packet. Indeed, in our proposal, the neighbor devices authenticate each other by checking the shared key used to encrypt the received packet. However, in SAODV no mutual authentication is achieved.

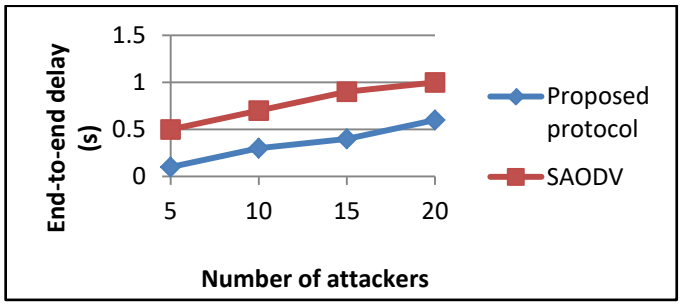

Fig. 1. End-to-end Delay Versus Numbers of Attackers.

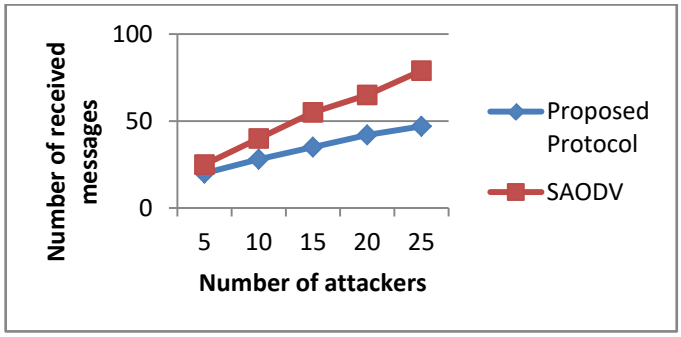

Fig. 2. Overhead Versus Number of Attackers.

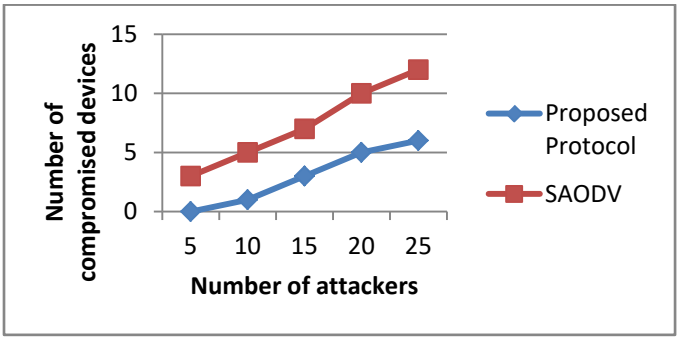

Fig. 3. Number of Compromised Devices Versus Number of Attackers.

Fig. 3 shows the results of the number of compromised devices as a function of the number of attackers. As we can see, the number of compromised devices in our proposed protocol is very less than SAODV protocol. This is because in our proposal when a device is compromised, only its private key is also compromised. The other devices are not affected, as the attacker cannot perform a mutual authentication with them because it cannot compute shared keys with these legitimate devices. However, in SAODV protocol from a compromised device, an attacker can compromise also its neighbor devices as the mutual authentication is achieved only between the source and the destination.

VI. Conclusion and Future Work

The special characteristics of the MWNs have a major impact on the security of routing data between the communicants. Indeed, secure a routing protocol in this type of network is exposed to many challenges like the limited battery of the devices and their small memories. Moreover, the routing is performed hop by hop through ordinaries nodes, so an attacker can easily compromise some nodes and participate in the selected route. In this context, we have proposed a secure and optimal routing protocol for MWN. This proposal takes into consideration the battery life of the intermediate devices that participate in the selected route. Moreover, security requirements like the confidentiality and authenticity are achieved during the routing process based on a proposed key-agreement method. Integrity is also achieved through the verification of the MAC function. To secure the request phase, we assumed that the neighbor devices compute shared keys between each other based on Weil Pairing scheme. To secure the data transmission phase, the source and the destination share a secret key where the parameters exchanged during the request phase. In this proposed protocol, we tried to fit inexpensive cryptography mechanisms in each phase to make it robust against many types of attacks.

As a future work, we plan to integrate an intrusion detection system to detect the malicious nodes and so to improve more the security in MWNs.

Acknowledgment

The author gratefully acknowledge the approval and the support of this research study by the grant no SAT-2018-3-9-F-7704 from the Deanship of Scientific Research at Northern Border University, Arar, K.S.A.

REFERENCES

[1] S. Corson and J. Macker, "Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Consideration", http://www.ietf.org/rfc/rfc2501.txt.

[2] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)", RFC 3626, October 2003.

[3] C. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers", Computer Communications Review, pp.234-244, October 1994.

[4] B. Liang and Z. J. Haas, "Hybrid Routing in Ad Hoc Networks with a Dynamic Virtual Backbone", IEEE Transactions on Wireless Communications, vol. 5, No. 6, pp. 1-14, June 2006.

[5] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad-Hoc Wireless Networking", in Mobile Computing, T. Imielinski and H. Korth, editors, Kluwer Academic Publishing, 1996.

[6] C. Perkins, E. M. Royer and S. R. Das, "Ad Hoc On-Demand Distance Vector Routing (AODV)", RFC 3561, July 2003.

[7] H. Zhand, "A WSN Clustering Multi-Hop Routing Protocol Using Cellular Virtual Grid in IoT Environment", Mathematical Problems in Engineering, vol. 2020, pp. 1-7, 2020.

[8] S. Othmen, S. Asklany, M. Wahida, " Fuzzy Logic Based On-demand Routing Protocol for Multi-hop Cellular Networks (5G)", IJCSNS International Journal of Computer Science and Network Security, VOL.19 No.12, December 2019.

[9] R. E. Ahmed, " A Low-Overhead Multi-Hop Routing Protocol for D2D Communications in 5G", *Journal of Communications Vol. 16, No. 5, May 2021*.

[10] H. Khojima, N. Yanai and J. P. Cruz, " Improving the Security and Availability of Secure Routing Protocol", IEEE Access, Vol. 7, pp. 1-20, May,13, 2019.

[11] G. Singh, H. Rohil, R. Rishi and V. Ranga, "International Journal of Engineering and Advanced Technology (IJEAT)", Vol. 9, pp. 498-504, Octobor, 2019.

[12] A. Bhusari, P.M. Jawandhiya and V.M.Thakare, "Optimizing performance of Anonymity based Secure Routing Protocol utilizing Cross layer Design for Mobile Adhoc Networks", Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), pp. 1-6, 2018.

[13] A. Vinitha, M.S.S. Rukmini and Dhirajsunehra, "Secure and energy aware multi-hop routing protocol in WSN using Taylor-based hybrid optimization algorithm", Journal of King Saud University Computer and Information Sciences, vol. 2019, pp. 1-12, 2019.

[14] Khaled Hamouid, Salwa Othmen and Amine Barkat, "LSTR: Lightweight and Secure Tree-Based Routing for Wireless Sensor Networks", Wireless Personal Communications, vol. 2020, pp. 1-22, 22 January 2020.

[15] M. G. Zapata, "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing", ACM SIGMOBILE Mobile Computing and Communications Review, vol 6, pp. 06-107, July 2005.

[16] M. Sirajuddin, Ch. Rupa, C. Lwendi and C. Biamba, "TBSMR: A Trust-Based Secure Multipath Routing Protocol for Enhancing the QoS of the Mobile Ad Hoc Network", Security and Communcation Networks, vol 2021, pp. 1-9, April 2021.

[17] Boneh, D and Franklin, M. K., " Identity-based encryption from the Weil pairing. In 21st annual international cryptology conference advances in cryptology—CRYPTO 2001, Santa Barbara, California, USA, August 19–23, Proceedings, pp. 213–229, 2001.