Securing a mobile ad hoc NETwork against the man in the middle attack

Ryma Abass [a,1,*], Aimable Habyarimana [b], Karim Tamine [c]

[a] SUP'Com, University of Carthage, Tunis, Tunisia
[b] CAPGEMINI, Paris, France
[c] XLIM, Limoges University, France
[1] ryma.abassi@supcom.tn*, [2] ahmana@gmail.com, [b] ktamine@gmail.com
* corresponding author

ARTICLE INFO

Article history
Received: 2022-02-17
Revised: 2022-05-21
Accepted: 2022-06-17
Published: 2022-07-20

Keywords
NETworks
Wireles
MIM
MANET

ABSTRACT

Mobile Ad hoc NETworks (MANET) are a special kind of wireless networks where there is neither centralized authority nor pre-existing infrastructure. Hence, in such situation, authenticating nodes becomes a challenging task. This is even more true that some nodes may be tempted by spoofing other nodes identity in order to gain some rights and privileges. In such context, a protocol based on keys exchange such as Diffie-Hellman can be used. However, even such protocol is vulnerable to impersonation attack e.g. the Man in the Middle (MIM) attack. The main objective of this work is then, to evaluate the impact of a MIM attack on the context of MANET and to propose a security solution to such situation. This is done by (1) estimating the needed ratio of attackers to achieve a MIM attack in a given MANET and (2) proposing a security process based on the well known Diffie-Helman protocol.

1. Introduction

Mobile Ad hoc NETworks (MANET) [1] are wireless mobile nodes dynamically self organizing in arbitrary and temporary network topologies and without a pre- existing communication infrastructure. Therefore, such networks are designed to operate in widely varying environments, from military networks to low-power sen- sor networks and other embedded systems. Dynamic topologies, bandwidth con- straints, energy-constrained operations, wireless vulnerabilities, and limited secu- rity are among the main MANET characteristics.

Securing MANET appears then as a challenging task particularly because of the specifications of these networks such as introduced previously [2]. In fact, some nodes may be tempted to falsify messages in order to disturb exchanges or to spoof other identities in order to benefit from some privileges. For instance, authentication achieved using keys exchange is vulnerable to the Man in the Middle attack (MIM).

Our main concern in this paper is then two fold. First, we estimate the ratio of colluding attackers needed to achieve a succesful MIM attack in a given MANET. More precisely, we are interested by the MIM that can be used by attackers in order to impersonate benevolent nodes and to intercept all relevant messages passing between the victims and inject new ones. Second, we propose a new protocol countering the MIM attack in such situation and based on the well known Diffie- Helman (DH). Diffie-Hellman is a powerful algorithm for secure keys exchange over a insecure channels. It was originally conceptualized by Ralph Merkle [3] and designed in its actual version by Diffie and

Hellman [4]. It allows two participants, which have no prior knowledge of each other to establish a common secret key. Thus, this key can be used to encrypt further communications. However, the DH protocol is vulnerable to a MIM attack. Hence, we propose a new variant of DH in order to withstand the MIM attack.

The remaining part of this paper is structured as follows: Section 2 reviews some existing works. Section 3 presents the MIM attack in the context of a MANET. This is done using a performance evaluation. Section 4 is concerned with the main contribution of this paper: a proposal securing MANET against the MIM attack. In Section 5, we present some simulation experiments and results showing the proposal performances. Finally, section 6 concludes this paper by summarizing its main contributions.

2. Related Work

After reviewing works dealing with keys management in MANET, we foundthat existing protocols can be classified intofiveclasses: (1) protocols based on partially distributed certification authority (2) protocols based on completely distributed certification authority (3) protocols based on certificates chaining (4) cluster based approachs (5) identity based protocols such as described by Table 1.

Protocols based on partially distributed certification authority distribute trust among a subset of communicating nodes in the network [5], [6]. In [6], authors employ threshold cryptography to distribute the CA functionality over specially selected nodes based on security and physical characteristics of the nodes.In [5], all nodes in the system know the public key of the service and trust any certificates signed using the corresponding private key. Nodes, as clients, can submit query requests to get other clients' public keys or submit update requests to change their own public keys. Hence, problems inherent to the absence of central authority are eliminated. However, revocation is not handled.

In protocols based on totally distributed certification authority, keys manage- ment is handled by all the nodes of the network . In [7], authors proposed a local- ized trust model, together with its realization to address issues of ad hoc wireless networks such as node mobility, network dynamics, wireless channel errors, DoS attacks and adversary break-ins. More precisely, in the proposed localized trust model, an entity is trusted if any k trusted entities claim so within a certain time period $Tcert$. These k entities are typically among the entity's one-hop neighbors.

Once a node is trusted by its local community, it is globally accepted as a trusted node. Otherwise, a locally distrusted entity is regarded as untrustworthy in the entire network. k and $Tcert$ are two important parameters with $Tcert$ characterizing the time-varying feature of a trust relationship. The main advantage of such model is that the charge is equitably distributed among all the nodes of the network. How- ever, it is inadequate for totally self organized MANET since any new node needs an initial certificate before it joins the network. This certificate is generated by an offline trusted authority.

Using certificates chaining, communicating nodes authenticate certificates as follows. A node A having to communicate with node C has to authenticate its certificate. A and C didn't communicate before however node A approved node B^Js certificate and B approved C^Js certificate. Hence, A approved C^Js certificate based on B^Js recommendation.A certificate chain is then constituted between A, b and C. In [8], authorsproposed a fully self-organized public-key managementsystem that allows users to generate their public-private key pairs, to issue certificates, and to perform authentication regardless of the network partitions and without any centralized services. Furthermore, this approach does not require any trusted authority, not even in the system initialization phase. Hence, key authentication is performed via chains of Public Key certificates in the following way. When a user u wants to obtain the Public Key of another user v, he acquires a chain of valid public-key certificates such that: (1) the first certificate of the chain can be directly verified by u, by using a public key that u holds and trusts (2) each remaining certificate can be verified using the public key contained in the previous certificate of the chain (3) The last certificate contains the public key of the target user v. Finally, to correctly perform authentication via a certificate chain, a node needs to check that all the certificates on the chain are valid and all the certificates on the chain are correct. However, such approaches are expensive in terms of computation and communication overhead.

Identity based protocols [9]–[11] use the same concepts as partially dis- tributed systems and add cryptographic system based on identity in order to reduce storage of publics keys. In (9), a group of trusted nodes distributes cryptographic material only if a subset of that group agrees on the trustworthiness of new mem- bers. More precisely, a master public key PK^* is generated by participating nodes. The master secret key $SK^*$is shared in a $t-out-of-n$ threshold manner by this initial set of n nodes. The main advantage of such approaches is that private keys are short and easy to generate and store, public keys are implicitly carried by their identities, so there is no need to distribute and store certificates of partners or public key of CA [11].

Clusters based protocols [12] are based on clustering algorithms dividing the networks into small groups. Each group member can then monitors its neighbors and recommends them to other clusters members, too. Clustering has been proven effective in minimizing the amount of storage for communication information and in optimizing the use of network bandwidth. Hence, in [12], authors divided the network into different regions with a similar number of hosts in each region. Nodes clustered together in the same region form a group and are assigned a unique group ID. Since a mobile ad hoc network has no centralized server for trust and key management, they defined a fully distributed trust management algorithm to maintain network security where any user can act as a certifying authority meaning that any node can sign the public key certificate of another node in the same group upon request.

Table 1. Comparison of related works

Approach	Characteristics	Advantages	Disadvantages
Partially distributed certification authority (5; 6)	Key management is handled by a sub set of communicating nodes	no centralized authority	no certificates revocation
Completely distributed certification authority (7)	Key management is handled by all communicating nodes of the network	charge is equally distributed between nodes	inadequate to the MANET totally auto-organized due to the intial certificates that must be generated before the network constitution.
Certificates chaining (8)	Each node generates its own certificates for other nodes	suitable for totally self-organized MANET	expensive in terms of computation and communication overhead
Cluster based (12)	Divides the network into groups (clusters) where each node is in charge of monitoring its neighbors and recommending their certificates.	routing is simplified	clusters maintenance is difficult due to the dynamic nature of MANET. CH constitute the main vulnerability of such configuration.
Identity based (9; 10; 11)	Uses an identity based crypto system to reduce the storage need compared with traditional PKI	Easier to deploy without any infrastructure requirement. Its resource requirements, regarding process power, storage space, communication bandwidth, are much lower.	vulnerable to the MIM attack for new nodes joigning the network

3. Evaluating the Man In the Middle attack in the context of MANET

Diffie-Hellman is a powerful algorithm for secure keys exchange over insecure chan- nels. It allows two nodes A and B, which have no prior knowledge of each other to establish a common secret key that can be used to encrypt further communications as follows:

- A and B pick g and p that are public such that g < p and g is a primitive root modulo p.
- A picks a secret integer a such that 0 ≤ a ≤ p-1 computes $X = g^a mod(p)$ and sends X to B.
- B picks a secret integer b such that 0 ≤ b ≤ p-1, computes $Y = g^b mod(p)$ and sends Y to A.

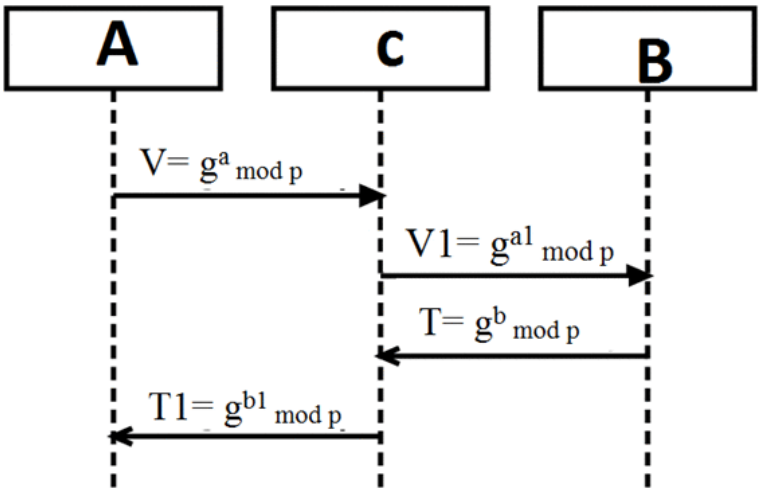

Fig. 1. MIM attack enforcement

- Both A and B can now compute respectively the key $K = Y^a mod(p) = X^b mod(p)$

However, the DH protocol is vulnerable to a Man In the Middle (MIM) attack. This will be detailed in the following.

3.1. MIM attack

Figure 1 details the considered MIM attack enforcement.

Let us consider p∈ Z/pZ (p a prime) and the generator g ∈ Z/pZ as public values. A and B are exchanging secret whereas attacker C is intercepting public keys and trying to construct false ones. These latter will be used in order to crypt and decrypt exchanged messages between A and B.

- A and B pick g and p that are public such that $g < p$ and g is a primitive root modulo p.
- A picks a secret integer a such that 0 ≤ a ≤ p-1
- B picks a secret integer b such that 0 ≤ b ≤ p-1
- C picks two integers $a1$ and $b1$ such that 0 ≤ a1, b1≤ p-1
- A tries to send the value g^a to B, C intercepts the value g^a
- C sends g^{a1} to B then B computes $K_1 = (g^{a1})^b = g^{a1b} = (g^b)^{a1}$
- B tries to send the value g^b to A, C intercepts the value g^b
- C sends g^{b1} to A then A computes $K_2 = (g^{b1})^a = g^{b1a} = (g^a)^{b1}$

The attacker C who chose $a1$ and $b1$, and intercepted g^a and g^b, becomes able to compute K_1 and K_2.

Consequently, A and C share the key K1 whereas nodes B and C share key K2 meaning that the attack has succeeded.

Used keys in this attack are formalized as follows:

$K_1 = V\,1^b \bmod p = g^{a1b} \bmod p = T^{a1} \bmod p.$
$K_2 = T\,1^a \bmod p = g^{b1a} \bmod p = V^{b1} \bmod p.$

3.2. Performance evaluation

In the previous section, we showed that the Diffie-Hellman protocol is vulnerable to a MIM attack for the case of two nodes exchanging a secret. But what about a dynamic, mobile and autonomous collection of nodes (network)? This is our con- cern in this subsection: depicting the MIM impact on a MANET. More precisely, we consider a coalition of attackers trying to pick up an exchanged secret based on the Diffie-Helmann protocol.

Used simulation parameters are listed in Table 2.

Table 2. Simulation Parameters

Parameter	Value
Simulator	NS 3
Nodes number	20-100
Mobility	Random-Waypoint Model 5 m/s to 30 m/s with a pause time = 0.2s
Propagation Model	FRIIS
Routing Protocol	AODV
Attackers	chosen randomly
Simulation time	100 sec

Moreover, the following hypotheses were used:

- Attackers constitute a coalition.
- Senders and receivers are chosen randomly.
- n secrets (n packets) are exchanged from n senders to n destinations meaning that each sender sends only one packet to a given destination.
- Only nodes having received successfully a packet can respond.

Two cases are then conceivable:

- The secret can be intercepted when sent from the sender node to the receiver node and intercepted in the other direction, too. In such case, the rate of MIM attack can be calculated.
- The secret can be intercepted only in one direction (outward or return). In such case, the rate of DoS attack can be calculated.

Moreover, having k pairs of randomly chosen nodes communicating, let us consider the following sets

- C: list of k_1 received packets among the k sent such that $k_1 \leq k$.
- D: list of intercepted packets by the coalition among the k_1 received ones.
- A: list of k_2 packets received by sources nodes among the k_1 sent by the k_1
- destination nodes such that $k_2 \leq k_1$.
- B: list of intercepted packets by the coalition among the k_2 received packets.
- $E = B \cap D$: list of packets received by the coalition in outward and return directions.
- $F1 = B \setminus E$: list of intercepted packets by the coalition in the outward direction.
- $F2 = (D \cap A) \setminus E$: list of intercepted packets in the outward direction, received in the return direction and non intercepted in the return direction.

Hence, the MIM attack ratio is obtained by Equation 1 :

(1)

$$\%\text{MIM} = \frac{\text{card(E)}}{\text{card(A)}}$$

3.3. Results and discussion

Several simulations were made in order to evaluate the impact of the MIM attack on a MANET.In the first simulation, we varied the nodes numbers from N = 30 to N = 100, fixed the numbers of pairs exchanging secrets k = 100 and varied the ratio of attackers 0% ≤ p ≤ 50%. Obtained results are depicted in Figure 2. Let us note that this figure is obtained for the smallest value of p needed to have a successfull MIM attack.

According to this Figure, when the coalition nodes ratio is around 20%, the probability of the success of the MIM attack is around 100%. Moreover, when N= 90 , the MIM attack is successful for 10% of attackers. Hence, the minimal ratio of attackers for a successful MIM is around 20%.

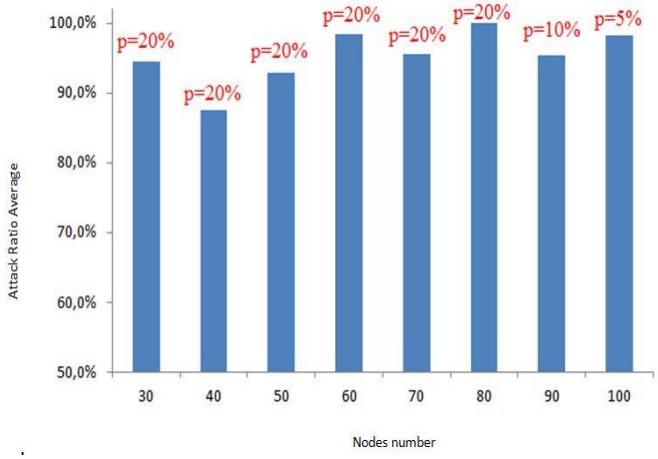

Fig. 2. Evaluation of the nodes number for a successful coalition

In the second simulations, we used three values of p : p = 10%; p = 20%; and p = 30% as well as two variation of N :N = 70 *then* N = 100. For each N and p, we considered ten values of k (k = 10; k = 20; k = 30; ...; k = 100) and we observed the number of pairs where the attack appears. Obtained results are depicted in Figure 3 and Figure 4.

According to these two figures, the greater the nodes pairs exchanging secrets, the greater the probability of a successful attack for a given N and a given p.

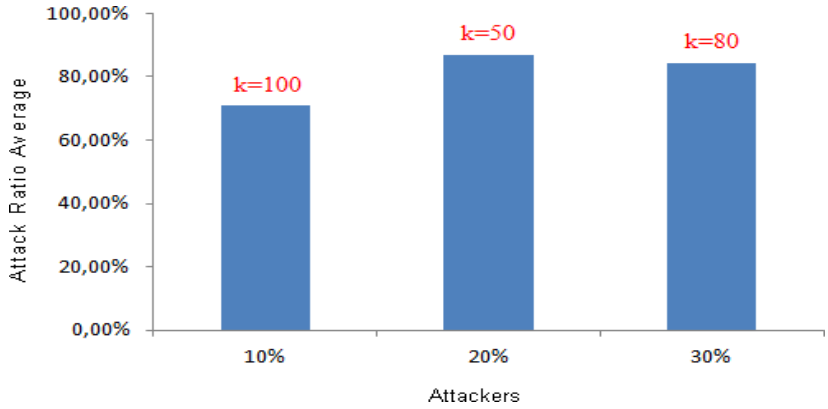

Fig. 3. Pairs numbers for a successful attack, N=70

Based on the two previous simulations, we investigate in the third one whether the value of N can increase or decrease the probability of the success of the attack. Hence, for each N , p where fixed to 10%, 20%, 30%, 40% and 50% and K = 100 .

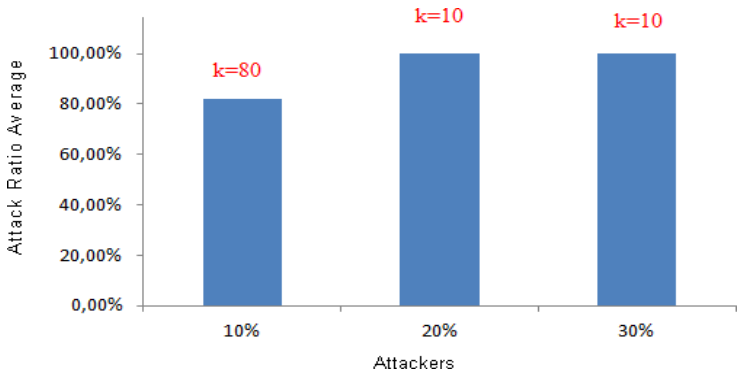

Fig. 4. Pairs numbers for a successful attack, N=100

Obtained results are depicted in Figure 5.

As one can see, the MIM attack is more easier to be done in a network with a great number of nodes with p% of attackers (p < 30%) than in a network with few nodes.

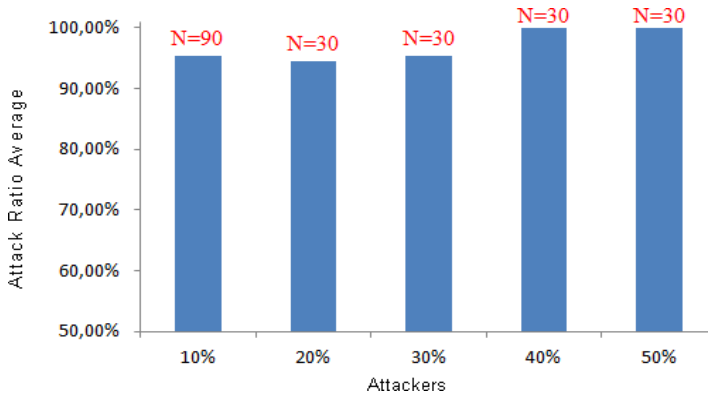

Fig. 5. Nodes number for a successful attack

4. Securing MANET against the MIM attack

As demonstrated in the previous section, the DH protocol is vulnerable to a MIM attack where the rate of colluders is around 20%. Hence, in this section, we present our main contribution: a secure exchange protocol for the DH protocol.

4.1 Proposal

The main idea is to send public key several times separated by a time interval T great enough to be sure that the network topology was changed. This constraint will ensure that two consecutive sent keys will not be routed using the same route. In fact, T must be carefully chosen in order to be sure that the topology has been changed increasing by the fact the probability of having different paths for successively sent packets. For instance, if packet pi is intercepted by a colluder, we must be able to prevent packet pi+1from being interceptd by the same colluder (the topology wasn't changed).

Having that in a MANET with DH protocol each received packet can be either sent by the legitimate source or by an attacker, each node will constitute two packets' lists: A and B. In fact, each received packet can contain either the value L (i.e. legitimate packet) or a different value (forged packet). In the following we associate list A to legitimate packets whereas the list B is associated to forged packets. Consequently, our proposal must be able to choose the key in the list A which can be guaranteed if $cardinal(A) > cardinal(B)$. In such case, the colluder will not be able to reply the DH protocol since each node has the ability to choose the legitimate key (g^a or g^b) which is contained in list A. Let's recall that a MIM attacker can only modify intercepted packets in order to compute the key. Hence, our protocol can choose to use tha value contained in list A or B.

The whole proposal can be formalized as follows:

1 A and B picks g and p that are public such that $g < p$ and g is a primitive root modulo p.

2 A picks a secret integer a such that 0 ™ a ™ $p - 1$, computes $X = g^a mod(p)$,

(a) sends X to B, waits T seconds,

(b) sends X to B, waits T seconds,

(c)….

(n) sends X to B.

1. B picks a secret integer b such that 0 ™ b ™ $p - 1$, computes $Y = g^b mod(p)$,

(a) sends Y to A, waits T seconds,

(b) sends Y to A,...., waits T seconds,

(c) .....

(n) sends Y to A.

1 Both A and B when receiving X and Y respectively, increment CA, assign $Val = X$ respectively $Val_i = Y$

2 For each value of X or Y received later,

(a) if the received value Val_i is equal to the Val, then increment CAelse incre- ment CB and assign $Val_B = Val_i$

(b)if $CA < CB$ then return Val_B else return Val else return failure

3 $K = Y^a mod(p) = X^b mod(p)$

4.2 Simulations and results

The aim of the following section is to study the performance of the proposition by a simulation work. This latter is used to show that our proposal is resistant to a MIM attack evn in presence of colluders. More precisely, we investigated the highest colluders rate in the network for which card(A) > card(B) showing by the fact the efficiency of our proposal since the exchanged values are safe.

Used parameters are depicted by Figure 3 where one can note that we used T = 3s. In fact, before simulating our proposal, we determinated the value of the interval T and after several simulations, we observed that the MANET topology changes completely after 2.8 s. Since we are using the Random-Way point Model with a pause time equals to 0.2s, we considered T = 3s.

Table 3. Simulation Parameters

Parameter	Value
Simulator	NS 3
Nodes number	50; 60; 70; 100
Mobility	Random-Waypoint Model 5 m/s to 30 m/s with a pause time = 0.2s
Interval between packets	30s
Nodes Pairs exchanging secrets	50
Propagation Model	FRIIS
Routing Protocol	AODV
Attackers	chosen randomly
Simulation time	100 sec

Let us note by INT the intercepted packets and by TR, the total of received packets.

In order to evaluate this protocol, the two conditions introduced previously and allowing us to choose the appropriate value to be used were highlighted (INT < 50%TR and INT ≥ 50%TR).

Obtained results are depicted by Figure 6 aand Figure 7.

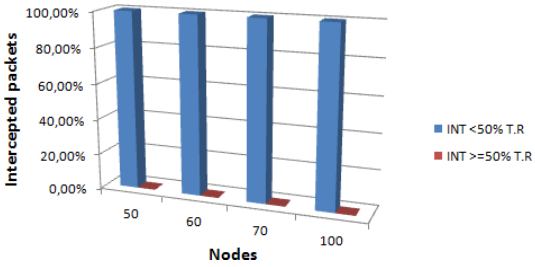

Fig. 6. Intercepted packets varying with the nodes number, p=10%

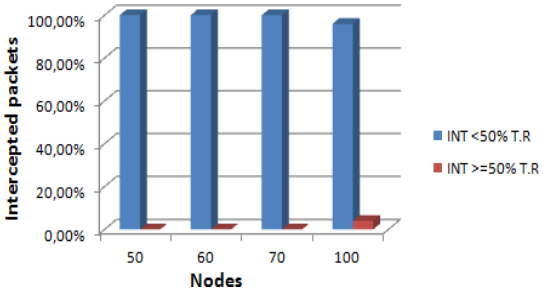

Fig. 7. Intercepted packets varying with the nodes number, p=20%

As we can note, our proposal is efficient for a MANET where 20% of the nodes are attackers whereas when this percentage reachs 30%, the proposal becomes less efficient.

5. Conclusion

In this work we are concerned by safely exchanging information in a MANET environment where colluders are achieving a MIM attack. More precisely, our con- tribution is two-folds. First, we evaluated the needed threshold of colluding nodes achieving a MIM attack in a MANET. This evaluation was made using NS3 sim- ulations with three parameters: the total number of nodes, the number of pairs using the DH protocol and the percentage of colluding nodes. Second, we proposed a security solution for such context based on the Diffie Helmann Protocol and thus by sending several times the same information during a given time interval.

Obtained results showed that a percentage of 20% of colluding nodes is needed in order to achieve a MIM attack in a MANET whereas the evaluation of our proposal shows that it is efficient as long as the colluding nodes represent less than 30% in the MANET.

References

[1] R. Abassi, "Trust management in mobile ad hoc networks for qos enhancing," in *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*, IGI Global, 2015, pp. 131–161.

[2] S. Kaushik and M. Kaushik, "Analysis of MANET security, architecture and assessment," *Int. J. Electron. Comput. Sci. Eng. (IJECSE, ISSN 2277-1956)*, vol. 1, no. 02, pp. 787–793, 2012.

[3] R. C. Merkle, "Secure communications over insecure channels," *Commun. ACM*, vol. 21, no. 4, pp. 294–299, 1978.

[4] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[5] S. Yi and R. Kravets, "Key management for heterogeneous ad hoc wireless networks," in *10th IEEE International Conference on Network Protocols, 2002. Proceedings.*, 2002, pp. 202–203.

[6] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE Netw.*, vol. 13, no. 6, pp. 24–30, 1999.

[7] H. Luo, P. Zerfos, J. Kong, S. Lu, and L. Zhang, "Self-securing ad hoc wireless networks.," in *ISCC*, 2002, vol. 2, pp. 548–555.

[8] S. Capkun, L. Buttyan, and J.-P. Hubaux, "Self-organized public-key management for mobile ad hoc networks," *IEEE Trans. Mob. Comput.*, vol. 2, no. 1, pp. 52–64, 2003.

[9] A. Khalili, J. Katz, and W. A. Arbaugh, "Toward secure key distribution in truly ad-hoc networks," in *2003 Symposium on Applications and the Internet Workshops, 2003. Proceedings.*, 2003, pp. 342–346.

[10] S. Honarbakhsh, L. B. A. Latif, and B. Emami, "Enhancing security for mobile ad hoc networks by using identity based cryptography," *Int. J. Comput. Commun. Eng.*, vol. 3, no. 1, p. 41, 2014.

[11] S. Zhao, A. Aggarwal, R. Frost, and X. Bai, "A survey of applications of identity-based cryptography in mobile ad-hoc networks," *IEEE Commun. Surv. tutorials*, vol. 14, no. 2, pp. 380–400, 2011.

[12] E. C. H. Ngai, M. R. Lyu, and R. T. Chin, "An authentication service against dishonest users in mobile ad hoc networks," in *2004 IEEE Aerospace Conference Proceedings (IEEE Cat. No. 04TH8720)*, 2004, vol. 2, pp. 1275–1285.