Secure Routing Protocol based on Weil Paring for Multi-hop Cellular Network (SRP-MCN)

Salwa Othmen[1], Faouzi Zarai[1], Aymen Belghith[2],Lotfi Kamoun[1]
[1]LETI laboratory, University of Sfax, Tunisia
[2]University of Sfax, Road of Aeroport Km 0.5, 3029 Sfax, Tunisia

Abstract
Nowadays, many advanced are developed and become available for users. So, the demand for a higher data rate wireless access significantly increases. For that reason, new cellular wireless networks have been introduced such as Long Term Evolution (LTE), LTE-advanced and Worldwide Interoperability for Microwave Access (WiMAX). However, the centralized topology of these technologies requires that the users have a direct connection to the Base Station (BS). Such topology suffers from many limitations such as congestion problem when a large number of users are communicating at the same time with the BS. In this context, the Device-to-device and the mobile relays communications have been proposed to overcome the limitations of the conventional cellular architecture. So, the key building block of the Multi-hop Cellular Networks (MCNs) is the multi-hop routing of data from the source to its target destination. In this paper, we propose a new Secure Routing Protocol for Multi-hop Cellular Networks (SRP-MCN). The goal of the proposed work is to discover secure and short routes between the source and its target destination in a secure way. To analyze and validate our proposed scheme, some simulations are performed based on Network Simulator (NS-2). The obtained validation results show that our proposed scheme outperforms the existing protocol named Anonymous and Authenticated Routing Protocol for Multi-hop Cellular Networks (AAR-MCN) in terms of end-to-end delay, throughput and Normalized Routing Load (NRL).

Keywords
component; LTE, WiMAX, MCNs, routing, security;

I. Introduction

In traditional single hop cellular networks, the mobile stations can communicate with each other only through the Base Station (BS). Such architecture suffers from many problems such as the high signal attenuation especially when the station is at the edge of the cell. In order to partially overcome this problem, installing a high number of BSs is required. However, increasing the infrastructure of such networks is very expensive at management and deployment phases. Other emerging alternative called Multi-hop Cellular Networks (MCNs) is currently considered as a part of the fifth Generation (5G) network evolution. It includes the integration of cellular and Ad-Hoc technologies [1]. This alternative has a lower implementation cost in comparison with adding new BSs. Indeed, in this new technology the direct link between the mobile stations and the BSs is not required. So, they can communicate with each other directly without any relay. Many studies have showed the advantages and benefits provided by MCNs over traditional single hop cellular networks. Indeed, the coverage area [2] and the transmission rate can be increased due to the reduction of the signal loss in each mobile [3]. As the signal covers a small distance, the energy consumption of each node is also reduced [4]. However, exploiting the mobile stations communications capabilities in a distributed and decentralized manner represent an important challenge for MCNs. For that reason, it is necessary to take into consideration some important technological challenges such as design and secure multi-hop routing protocols. Two cases of communication are distinguished in MCNs. The first case is when the source and the target destination are in the same cell. In this case, the packets are relayed by the mobile terminals and the intervention of the BSs is not required. However, when the source and the destination are in different cells, the BSs have to participate in the routing process. Indeed, when a source wants to communicate with a destination, it sends the packets to its associated BS through multi-hop relays. Then, this BS forwards the packets through the associated BS of the destination. The routing protocols proposed in the literature for the Ad Hoc networks can be applied when the source and the target destination are in the same cell [5-9].

Two cases of communication are distinguished in MCNs. The first case is when the source and the target destination are in the same cell. In this case, the packets are relayed by the mobile terminals and the intervention of the base station is not required. However, when the source and the destination are in different cells, the BSs have to participate in the routing process. Indeed, when a source wants to communicate with a destination, it sends the packets to its associated base station through multi-hop relays. Then, this BS forwards the packets through the associated BS of the destination. The routing protocols proposed in the literature for the Ad Hoc networks can be applied when the source and the target destination are in the same cell [4, 5]. However, the routing process between two different cells is more complicated because the presence of the base station and the backbone has to be

Manuscript received June 5, 2016
Manuscript revised June 20, 2016

considered. In order to enhance routing in MCN, other adaptable routing protocols are proposed. However, securing these proposed protocols is an important challenge due to the participation of the mobile nodes in the routing process.

For the best of our knowledge, a few research works have been proposed in the security issue and countermeasure of routing protocol in MCN.

In this paper, we propose a new routing protocol for MCNs. This protocol selects secure and short routes that ensure security in terms of confidentiality, integrity and authentication. To achieve the anonymity of the users, temporary identities are used in the communication. Moreover, to minimize the computational overhead for a node in verifying the validity of node's certificate, we use the Smart-Chen-Kudla scheme [10]. This scheme can help each node to implicitly authenticate its neighbor with minimum complexity. To secure the exchanged data between them, the source and destination generate a session key initiated by the source node.

The paper is organized as follows. In section II, we present some related works of routing protocols for MCNs. In section III, we describe our proposed protocol in detail as well as some notations and assumptions used to achieve the desired goals. To evaluate its performance some analysis and simulation results based on Network Simulator (NS-2) [11] are given in section 5. We conclude the paper and present some proposed future works in the last section.

II. Related work

Many routing protocols are proposed in the literature for Ad Hoc networks. These protocols can be adapted for MCNs only when the source and its target destination are in the same cell. However, in the other case when the source and destination are in different cells, these protocols cannot be considered because they do not take into account the presence of the BSs in the routing decision.

In [12] M. Elsalih et al. proposed an anonymous and authenticated routing protocol for MCN (AAR-MCN). In this protocol before launching the route establishment phase, each mobile node must authenticate to the trusted party to get a dynamic identity and a symmetric key shared with the associated BS. Then, when a source node wants to communicate with a destination, it initiates a route discovery session by broadcasting a request packet (RREQ). This packet contains the latest dynamic identity of the source shared with the associated BS, the time to live (TTL) to bind the propagation area of the packet, and a padding (PD) chosen randomly to protect the location anonymity of the source. The length of this padding and the real identity of the destination are encrypted by the key shared between the source and the BS.

When an intermediate node receives the RREQ, it decrements the TTL value and adds its dynamic identity to this packet before broadcasting it to the next neighbors. By this way, the BS can authenticate all intermediate nodes when it receives the RREQ by verifying their temporary identities. Then, it generates a reply packet (RREP) and sends it back to the source. The RREP packet contains a part for each mobile node participating in the selected route. Each part includes the new dynamic identity of the node and a session key shared with its previous neighbor. When an intermediate node receives the RREP packet, it hashes the received key value to derive a new one shared with its next neighbor. Then, it takes off its part and broadcast the RREP packet until it reaches the source node. Finally, the BS sends to the BS associated with the destination (BSD) a call request in order to establish a route to the target destination. The BSD broadcasts an RREQ packet to its neighbor nodes. This packet is routed hop by hop until it reaches the destination. When, the destination receives the RREQ packet, it replies the BSD with an RREP packet via the reverse route. Each intermediate node of the selected route adds its new temporary identities to the RREP packet. Finally, when the BSD receives the RREP packet, it distributes a session keys shared between the nodes of the selected route. This proposed protocol is secured against some type of attacks such as the replay attack by using dynamic identities in each session and Sybil attack as the BS authenticates each intermediate node by checking its identity. However, this protocol suffers from many limitations. Indeed, it is not secured against impersonation attack. Moreover, integrity and authentication between nodes are not guaranteed. In [13] J.J. Haas et al. proposed a secure routing protocol for unified cellular Ad Hoc networks. This protocol is divided into two behaviors: downlink (from cell network to the node) and uplink (from the node to the cell network) behaviors. For the downlink behavior, first, the source node broadcasts a route request packet which contains its identity and its required throughput for data upload. When a neighbor node receives this packet, it checks if it can satisfy the throughput required by the source. If yes, it generates a route reply packet which contains its upload throughput and its identity. The source selects the more appropriate neighbor to route its data toward the BS based on the received replies (node with high value of upload throughput). Then, it establishes a shared secret key with this node and checks its legitimacy via the BS. It sends a data packet that includes the expected transmission time of a packet, the identity of this selected node and MACs code to cover the transmitted data. After receiving this packet, the BS checks the MACs code to authenticate the source, ensures that the expected transmission time has not expired and that the selected node is chosen by the source (not by an attacker). If the verification passes, the BS directly sends an acknowledgement to the source. The uplink behavior is performed with the same way as the downlink behavior but with additional stage at the end. When the BS receives a data packet to authenticate the source and its neighbor node, it generates a secret key between it and the source to secure the exchanged data.

The proposed protocol is secured against many types of attacks. Indeed, the MAC keyed with session key K provides data integrity and authenticates the source node by the BS in the downlink and uplink side. A protection against replay attack is achieved by the including of timestamp in data packet. However, this protocol suffers from some limitations. Indeed, the impersonation attack is possible and the participation of the BS in the authentication technique between nodes is expensive in terms of time. Moreover, both the route request and route reply include the identities of the source and its neighbor nodes in plaintext, so no anonymity is achieved.

In [14], J. Suresh et al. secured the routing of packets between nodes in MCNs by detecting the irrational nodes. Indeed, each transmitted packet is appended with a checksum. This value is computed at every hop. If a node checks the received packet and it finds a difference in the checksum value, it detects that the sender is an irrational node. In order to increase security in this protocol, the trivial hash function is used instead of hash function which needs more computation cost. Moreover, to reduce the collision problem a border node is chosen to submit the checks at the Accounting Center using a digital signature. This proposed protocol is secured against many attacks such as Sybil attack as an attacker cannot generate a true signature to falsify the Accounting Center. Also, this protocol guarantees integrity by using the trivial hash function. However, it is not secured against some type of attack such as impersonation attack.

III. Proposed Routing Protocol

A. Smart-Chen-Kudla Scheme

For key generation, our proposed protocol is based on "Smart-Chen-Kudla" scheme. In this scheme, the Trust Party (TP) is in charge of the generation and distribution of the public parameters ($q, H_1, P, P_{pub}, G1, G2$), where H_1 is a hash function $\{0, 1\}^* \rightarrow G1$, P is a generator of $G1$, P_{pub} is the master public key formed as $P_{pub} = sP$, where $s \in Zq$ is the master private key of the TP. The trusted party registers each mobile node M_i and assigned to it a master private key $P_i = s\ Q_i$, where $Q_i = H_1(ID_i)$ and ID_i is the identity of M_i.

When two communicants A and B want to share a secret key, each one generates a random value a and b respectively.

Key generation phase between A and B is performed as follows:

- A sends $T_A = aP$ to B,
- B sends $T_B = bP$ to A,
- A calculates its secret key as the following: $K_{AB} = H_2(abP \parallel \hat{e}(sQ_A, T_B)\hat{e}(Q_B, asP))$,
- B calculates its secret key as the following: $K_{BA} = H_2(abP \parallel \hat{e}(sQ_B, T_A)\hat{e}(QA, bsP))$,

Both users A and B share the same secret key:

$K = K_{AB} = K_{BA} = H_2(abP \mid\mid \hat{e}(bQ_A + aQ_B, sP))$

Where, H_2 can be a random oracle or a secure hash function.

B. Assumption

In our network model, we consider that:

- The source and destination are in different cells,
- TP generates and records the system parameters ($q, H_1, P, P_{pub}, G1, G2, s$) in a secure way.
- Before deployment, each new mobile station must authenticate to the TP via BS in order to obtain a private key $S_i = sQ_i$; Where $Q_i = H_1(ID_i||t)$, ID_i is the identifier of this node, s is the private key of the TP and t is a timestamp initiated by the TP to prevent the communication against the replay attack. After a fixed period, the nodes re-authenticate to the TP to obtain new private keys.
- Each mobile station M_i performs a neighbor discovery phase after a period of time in an authenticated way. During this phase, each node generates a random value (X_i) and sends to its neighbors the following value based on the Paring Discrete Logarithm Problem (PDLP) scheme:

  $P_i = X_i P$

C. Proposed Algorithm

When a source node wants to communicate with a destination localized in other cell, it broadcasts a RREQ packet to its neighbor nodes. This packet is relayed hop by hop until it reaches the BS_S. On receiving the RREQ, the BS_S sends a call request to the BS_D and sends back a reply to the source node. This phase is named uplink route discovery process. When the BS_D receives the call request, it replies the BS_S and broadcasts a RREQ packet to discover a route to the destination. This phase is called downlink route discovery process.

In the following section, we detail these two phases: Uplink and downlink route discovery processes.

1) Uplink Route Establishment

This phase is divided into the route request process and the route reply process:

➢ *Route Request Process*

In order to secure the RREQ packet, each mobile station M_1 computes a shared session key with the next node M_2

based on the Smart-Chen-Kudla scheme. This scheme is used to guarantee the confidentiality of the exchanged data as well as the authentication between nodes instead of verifying the certificate validity. This leads to minimize the expensive cryptographic mechanism in term of time and complexity. Also, to minimize computational complexity, the formula used in this proposed protocol is more efficient as the two communicants will perform only a single evaluation of the Weil Pairing [15] as compared with Smart-Chen-Kudla scheme.

M_1 generates a random number X_1 and computes the shared key with M_2 as the following equation:

$$\begin{aligned} K_{M1M2} &= \hat{e}\ (S_1; X_2Q_2 + X_1\ Q_2) \\ &= \hat{e}(sQ_1; X_2Q_2 + X_1\ Q_2) \\ &= \hat{e}\ (Q_1;Q_2)^{s(X_1+X_2)} \qquad (1) \end{aligned}$$

When M_2 receives this packet, it generates also a random value X_2 and computes the shared key with M_1 as the following function:

$$\begin{aligned} K_{M2M1} &= \hat{e}\ (X_1Q_1 + X_2\ Q_2\ ; S_2) \\ &= \hat{e}(X_1Q_1+X_2Q_2; sQ_2) \\ &= \hat{e}\ (Q_1;Q_2)^{s(X_1+X_2)} \qquad (2) \end{aligned}$$

M_1 and M_2 will obtain so the same key as follows:

$$K = K_{M1M2}= K_{M2M1}= \hat{e}\ (Q_1;Q_2)^{s(X_1+X_2)} \quad (3)$$

To achieve anonymity in our protocol, we assume that the nodes of the same route generate temporary identities in each session as follows:

$$XID_i = H_1(ID_i \| X_i) \qquad (4)$$

For that reason, we assume that the BS_S and the nodes in the networks are synchronized.

When a source S wants to communicate with a destination D, it initiates the route request process by sending a RREQ packet to its neighbors. The route request phase is performed as the following steps:

- **Step 1**: the source S generates and sends to its neighbors the RREQs packets.

  Step 1-1: S generates a random value r $\in Zq$ to compute a shared key with D. We propose to compute this key based on a random value generated only by S because the two communicants (S and D) are not neighbors so they cannot exchange random values to compute a shared key. Whereas, the other neighbor, each one sends a random value in the neighbor discovery phase to compute the keys shared between them. The random values are sent based on the logarithm discrete scheme for more security.

  Step 1-2: S generates the session key shared with D as follows:

  $$K_{SD}= \hat{e}(rP_S, H_1(ID_D)) \qquad (5)$$

  Step 1-3: S generates the session key shared with each neighbor M_i as equation (1).

  Step 1-4: S generates the *Padding* value which is a random bit string and its length is PL. This *Padding* added to protect the location anonymity of the source.

  Step 1-5: S generates a temporary identity

  $$XID_S = H_1(ID_S||X_S)$$

  Step 1-6: S generates the *Trapdoor*:{E (K_{SD}, $H_1(ID_D)$|| *r* || XID_S). This *Trapdoor* is a secret between the S and D, which is encrypted by K_{SD}, so that the intermediate node cannot know its content.

  Step 1-7: S sends to each neighbor M_i the packets RREQs: The format of RREQ packet is as follows: RREQ: {E (K_{Si}, XID_S|| E (K_{BS}, $H_1(ID_D)$)|| *seq_num* || *PD* || *PL* ||*TTL* || *Hop_count* || $rH_1(ID_S)$ || *Trapdoor*) || $H_2(*)$ }.

  The source adds to the RREQ packet its temporary identity XID_S. E (K_{BS}, $H_1(ID_D)$) is the identity of D encrypted by the public key of the BS for anonymity. *seq-num* aims to prevent the route request against reply attack. Time To Live (TTL) is used to limit the propagation area of the route request. *Hop_count* is the number of hops traversed by the route request and it is incremented by each hop. $rH_1(ID_S)$ is used by D to compute the shared key with S and $H_2(*)$ is the hashed value of the RREQ packet to ensure the integrity. If S does not receive a route reply in a defined time period, it sends a new RREQ packet. If it sends *k RREQ* packets without receiving any response from D, the source node records that this destination is unreachable.

- **Step 2**: Mobile station M_j receives a RREQ packet from its neighbor M_i. It performs the following subsets:

  Step 2-1: M_j decrypts the RREQ packet by the shared key with M_i. If the decryption is passed, the node M_i is authenticated by M_j because only these two nodes can compute this shared key.

  Step 2-2: M_j checks the integrity of the RREQ by computing its hash value. If the verification passes, go to step 2-3. Otherwise, discard this packet.

  Step 2-3: M_j checks *TTL* value. If it is equal to zero, it discards the RREQ packet. Otherwise, it decrements this value and increments the *hop_count* by one.

  Step 2-4: M_j generates a temporary identity as formula (4): $XID_j = H_1(ID_j \ || \ X_j)$ and adds it to the RREQ packet.

  Step 2-5: M_j records the identity of the previous node and removes it from RREQ packet.

  Step 2-6: M_j computes the hash value of RREQ.

  Step 2-7: M_j computes the shared key with each next neighbor M_k as equation (1).

  Step 2-8: M_j sends the RREQs packets to each neighbor protected by the shared corresponding key.

- **Step 3**: BS_S receives RREQs packets.

Step 3-1: BS_S decrypts the RREQs packets received through different routes.

Step 3-2: BS_S selects a fixed number of RREQs packets come from the shortest routes. We assume that BS_S chooses more than one route to avoid the re-initialization of the route request phases if the RREP of the selected route is dropped in the route reply.

Step 3-3: BS_S checks the integrity of this packet. If this verification passes, goes to Step 3-4. Otherwise, discard this packet, selects the second shortest route and goes to Step 3-4.

Step 3-4: BS_S decrypts the identity of D by its private key to decide the BS corresponding to this destination (BS_D).

Step 3-5: BS_S generates a call request packet (CRP) and sends it to BS_D. The format of call request is as the following: CRP: $\{ID_D \| seq\_num \| Trapdoor \| rH_1(ID_S) \}$

Step 3-6: BS_S lunches the route reply phase when it receives a response from BS_D. Otherwise, it sends an acknowledge packet to the source to indicate that D is unreachable.

Step 2-2: M_k checks the integrity of the RREP. If the verification passes, goes to step 2-3. Otherwise, it drops this packet.

Step 2-3: M_k maintains the temporary identity of the previous node and adds its temporary identity.

Step 2-4: M_k re-computes the hash value of RREP packet.

Step 2-5: M_k sends the RREP to the next node of the reverse route.

- **Step 3:** S decrypts the received RREPs, retrieves and records the temporary identity XID_D of D by decrypting it based on the shared key with the destination. S selects multiple routes among the received RREPs to communicate with D. If any problem is occurred, the source switches to the second shortest route maintained in its routing table without re-initialization of route request phase.

2) Downlink Route Establishment

After the BS_D receives the call request from BS_S, it triggers a route discovery phase by broadcasting a RREQ packet. When D receives this packet, it selects the shortest route and replies with the RREP packet.

➢ *Route Request Process*

After receiving a call request packet from BSS, the BSD generates and broadcast a RREQ packet to find a secure route toward D. Each node computes a secret key shared with its neighbors based on Smart-Chen-Kudla scheme. This key is used to secure the RREQs packets.

The format of RREQ packet sent by the node Mr to its neighbor Md is as follows:

$$\text{RREQ :}\{ E\ (K_{rd}, seq\_num \,\|\, PD \| \, PL \,\|\, TTL \| \text{ -}\ hop\_count_1 \,\|\, rH_1(ID_S) \,\|\, trapdoor), H_2(*)\}$$

Where, Krd is a secret key shared between Mr and Md, PD and PL are respectively the padding and its length generated by the BSD and the hop_count1 is the number of hops traversed by the RREQ.

The route request phase in the downlink behavior is performed as the route request in the uplink behavior described in the previous section. However, in the uplink route request, the source is not a mobile node it is the BSD which broadcasts the RREQ. This packet is sent hop by hop until it reaches the D.

➢ *Route Reply Process*

When D receives the first RREQ packet, it waits for a period of time the arrival of other packets. Then, it selects a fixed number of shortest routes based on the hop_count1 value and generates the corresponding RREP packet for each one. Then, it performs the same steps performed by the BSS in the route reply phase in the uplink behavior.

The destination compute the key shared with the source as the following equation:

$$\begin{aligned} K_{DS} &= \hat{e}\ (rH_1(\mathrm{ID}_S \| t), S_D\ ) \\ &= \hat{e}(r\ H_1(\mathrm{ID}_S \|\ t), sH_1(ID_D \| t)) \\ &= \hat{e}\ (r\ sH_1(\mathrm{ID}_S |\ t), H_1(ID_D \| t)) \\ &= \hat{e}(rS_S, H_1(ID_D \| t) \\ &= K_{SD} \end{aligned}$$

When BS_D receives the RREP from D, it sends a response to BS_S to inform it that it founds a secure route toward D.

IV. Analysis and Validation of our Proposed Routing Protocol

A. Analysis and Validation of our Proposed Routing Protocol

Confidentiality: The packets transmitted during the route establishment phase in the uplink and downlink behaviors are protected by the shared keys generated between each neighbors. These keys are generated using Smart-Chen-Kudla scheme based on several secret parameters such as the private key of TP. An attacker has to solve the Elliptic Curve Discrete Logarithm Problem (ECDLP) to find the secret key of the TP and compute the shared keys. Also, the source and the destination compute a session key shared between them and initiated by the source to protect the trapdoor. Nobody, except these two communicants can learn the content of the trapdoor. Because to learn the secret key an attacker must learn the private key of the destination.

Integrity: In the proposed protocol, each transmitted packet concatenates its hash value to provide integrity. To modify a packet, an attacker must decrypt its content and then computes the corresponding hash value of this modified packet. However, the decryption of such packet needs to learn the secret key shared with the sender. The shared keys and the private keys are generated using Smart-Chen-Kudla scheme or the cryptographic assumptions such as the ECDHP. By this way, the attacker cannot learn the correct keys to generate the corresponding hash value. So, the proposed protocol ensures the integrity of the transmitted data.

Authentication: In our proposed protocol, we are based on Smart-Chen-Kudla scheme for key generation. This scheme has the advantage to provide implicit authentication based on several secret parameters. Indeed, the TP generates for each node M_i a private key P_i using its identity. Based on this key, node M_i generates a secret key K_{ij} shared with its neighbor M_j. This node uses K_{ij} to authenticate M_i because; only a legitimate node can hold a private key containing the secret key of TP. Also, to authenticate each node in the route, the receiver checks the hash value of the received packet. The source and destination use the secret key K_{SD} shared between them to protect the trapdoor. Each one checks the trapdoor using K_{SD} to authenticate each other. An attacker cannot learn the secret key K_{SD} to forge the trapdoor and impersonate them because it is not able to learn the private keys and the identities of the source and the destination. Thus, our proposed protocol can achieve authentication.

Anonymity and Intractability: In the proposed protocol, each node participates in the route establishment phase using its on-time temporary identity. Based on this identity, an attacker is not able to reveal the corresponding real identity. Also, our anonymous routing protocol does not reveal the information related to the source, destination and the intermediate nodes. Even, these latter cannot learn with which node the source communicates. An attacker is not able to trace the RREQ packet based on its common parts to discover the source and the destination nodes because the RREQ is encrypted by the shared keys of the intermediate nodes. Also, it is difficult for an attacker to learn the possible source from the size of the RREQ because the size changes using random bit string padding for different routing requests. So, our proposed protocol provides anonymity and intractabilit**y**.

Key secrecy: The proposed protocol ensures perfect forward secrecy because when an attacker compromises the secret keys of all nodes, it cannot reveal the previous session keys. This is because each session key relies on random values.

Replay attack: In the replay attack, the attacker intercepts the authorized packets and retransmits them in order to falsify the destination. This attack cannot be realized in our proposed protocol because each session key is relay on random values generated by the two neighbor nodes. So, the new key will be generated without any links with the previous session key. Also, using the timestamp in computing a new temporary identity and a sequence number generated by the source for each new packet prevent our proposed protocol against replay attack.

Sybil attack: In the Sybil attack, the attacker generates some unauthorized identities and uses them to establish neighbor relationships with several legitimate nodes. These latter cannot determine that these false identities come from the same entity. In our proposed protocol, each node authenticates to the TP to obtain a private key corresponding to its identity and based on the private key s of the TP. So, to perform the Sybil attack, an adversary has to generate a private key for its false identity. This is not possible for an attacker because it must resolve ECDHP in order to learn the private key s of the TP. So, the Sybil attack is not possible in our proposed protocol.

Rushing attack: In the rushing attack, the attacker transmits the route request packet to a large number of nodes using a high transmission range. The receiver of this false packet may be unable to respond the sender, and so cannot establish the route. In our proposed protocol, when a node receives a request packet, it authenticates the sender of this packet by verifying the encryption key. If the authentication is performed successfully, the node accepts the packet and responds the sender because only an eligible node can generate a valid encryption key. So, if an attacker forwards a packet using a large transmission range, this packet will be not accepted by the receiver because it has not been authenticated. Therefore, the rushing attack cannot be realized in our proposed protocol.

Impersonation attack: In the impersonation attack, an attacker impersonates the identity of a legal node to establish a route with the other nodes in order to exchange messages with them or to establish a neighbor relationship. To perform this attack, an attacker must generate a secret key shared with the nodes to which it will send the message. However, using our proposed protocol, this attacker is not able to solve the ECDLP problem to learn the secret key of TP and computes a valid private key corresponding to this impersonated identity. Also, it is infeasible to learn the real identity of a legal node and compute its private key because the request packet does not contain a real identity of any node. Thus, the attacker fails to impersonate another legitimate node

B. Simulation Results

Our simulation scenario consists of two network densities with 20 nodes each one, placed randomly within

1000m*1000m area. Simulation time was 200 seconds. The MAC protocol used is IEEE 802.11 and the traffic type is the Constant Bit Rate (CBR) traffic. The packets size exchanged between sources and destinations is 512 bytes. Each source generates data packets continuously during the simulation time. Malicious nodes are placed and activated randomly in order to imitate arbitrary the nature of an attacker.

In order to assess our proposed protocol, it is compared with the Anonymous and Authenticated Routing in Multi-hop Cellular Networks (AAR-MCN) protocol (see the related works section). The performance metrics evaluated in our simulation scenario are defined as follows:

- Throughput is the average of data sent by the source and received by the destination during the simulation time.
- End-to-end delay is the average delay between the time of packet delivery to the target destination and the generation time of this packet.
- Normalized routing load (NRL) is the proportion between the number of routing packets transmitted during the simulation time and the number of data packets received.

The security techniques used in these two protocols such as encryption and hash functions are implemented using the crypto++ library as NS-2 does not support the cryptography tools. We also implement the black hole attacks in our proposed protocol and in AAR-MCN protocol.

Black hole attack [16] is a type of Denial of Service (DoS) attacks. In this attack, when a malicious node receives RREQs or RREPs packets it drops them and sends immediately a fake RREP to the source node. It can also forward it to the next node and try to become an intermediate node of the selected route. The source node can accept this packet received from the malicious nodes and so it drops all other RREPs. When it starts sending the data to the destination node using the route passes through the malicious node, this node can drop all packets or just analyze it to extract some important information, then it forwards it to the next node.

Figure 3 shows the end-to-end delay for our proposed protocol compared with the AAR-MCN protocol against the number of attackers. We note that SRP-MCN has the lowest delay and so provides better performance compared with AAR-MCN. This is because in our proposed protocol, each node authenticates each neighbor by checking the encryption key. If this verification does not pass, it drops this received packet directly and so no extra time spent by the other nodes to handle false packet. Moreover, with this authentication no way for an attacker to become a member of the selected route and increases the delay by spending more time to handle the received data to find helpful information.

As shown in figure 4, the increase of malicious nodes leads to a decrease in the throughput for both protocols. This is caused by the bad behavior of the malicious nodes during the simulation times as they drop some received packet. However, the SRP-MCN outperforms the AAR-MCN achieving more throughputs. This is because, in our proposed protocol each node authenticates its neighbors and so an attacker cannot become a member of the selected route to drop the received data. However, in the AAR-MCN the authentication is guarantee only between each node and the base station. So an attacker can trace a legal identity and participates in routing discovery process as a legitimate node to participate in the selected route.

Figure 5 shows the NRL parameter evaluated against the number of malicious nodes for SRP-MCN and AAR-MCN protocols. It is obvious that the NRL decreases when the number of malicious nodes increases as the attackers drop some received routing packets. However, the attackers cannot create a major impact in our proposed protocol as the nodes accept only the routing packets come from the legitimate nodes.

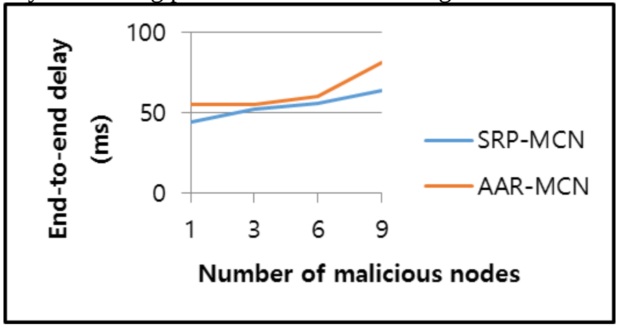

Fig.3. End-to-end delay versus the number of malicious nodes

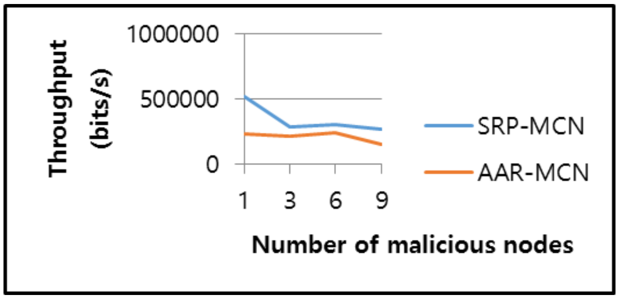

Fig.4. Throughput versus the number of malicious nodes

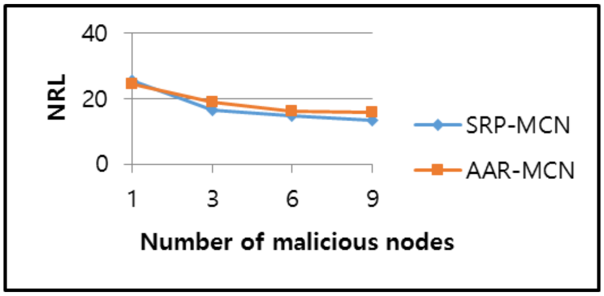

Fig.5. NRL versus the number of malicious nodes

V. conclusion

In Multi-hop Cellular Networks, the implementation of a reliable routing protocol which ensures both the network performance and the security requirement is a challenging task. In this article, we propose a secure routing protocol which selects the shortest path between a source and its target destination. This proposed protocol satisfies the security requirements in terms of confidentiality, integrity, authentication and anonymity. When designing this protocol, we try to adapt inexpensive cryptographic mechanism in each phase in order to make it robust against attacks. The route discovery process is secured by a shared key generated by each two adjacent nodes based on Smart-Chen-Kudla scheme. This scheme is used to guarantee the confidentiality of the exchanged data as well as the authentication between nodes instead of verifying the certificate validity. The integrity is guaranteed through the hashing technique. To ensure anonymity in our proposed protocol, we propose that the nodes exchange temporaries identities in each session based on the timestamp. The simulation results show that the proposed protocol satisfies a high throughput and less end-to-end delay and NRL in comparison with AAR-MCN protocol.
In the future work, we plan to extend this protocol to handle the case of node mobility between cells. In this case, we will analyze the impact of mobility on security especially that the mobile node will have new neighbors.

References

[1] Y. Lin and Y. Hsu, ``Multihop Cellular: A New Architecture for Wireless Communications'', pp 1273-1282, IEEE INFOCOM 2000.

[2] Y. Pei and Y. Liang, “Resource Allocation for Device-to-Device Communications Overlaying Two-Way CellularNetworks,” IEEE Transaction Wireless Communication, vol. 12, no.7, pp. 3611-3621, July 2013.

[3] P. Phunchongharn, E. Hossain, and D. I. Kim, “Resource Allocation for Device-to-Device Communications Underlaying LTE-Advanced Networks,” IEEE Wireless Communication, vol. 20, no. 4, pp. 91-100, August 2013.

[4] M. Kubisch, S. Mengesha, D. Hollos, H. Karl, and A. Wolisz, “Applying ad-hoc relaying to improve capacity, energy efficiency, and immission in infrastructure-based WLANs”. In Proceedings of communication in Verteilten System, Leipzig, February , Germany, 2003.

[5] C. Perkins, E. Belding-Royer and S. Das, “Ad Hoc On-demand Distance Vector (AODV) Routing, IETF RFC, 2003.

[6] D. Johnson, Y. Hu, Heinzelman and D. Maltz “The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4”, IETF RFC, 2007.

[7] S. Othmen, A. Belghith, F. Zarai and M. Oubaidat, “Power and delay aware routing protocol for Ad Hoc network”, IEEE International Conference on Computer and Information Technology (CIT), pp. 59-64, China, July. 2014.

[8] S. Othmen, A. Belghith, F. Zarai, M. Obaidat and L. Kamoun, “Power and Delay-aware Multi-Path Routing Protocol for Ad Hoc Networks, International Conference on Computer, Information and Telecommunication Systems (CITS), pp. 1-6, South Korea, July 2014

[9] M. G. Zapata, “Secure Ad hoc On-Demand Distance Vector (SAODV) Routing”, Internet DRAFT, 17 March 2005

[10] Smart, “N.P.: An identity based authenticated key agreement protocol based on the Weil pairing”,Electronic Letters, pp. 630– 632 , 2002.

[11] Network Simulator, http://www.isi.edu/nsnam/ns, last visited in May 2014.

[12] M. E. Mahmoud and X. Shen, “Anonymous and Authenticated Routing inMulti-hop Cellular Networks”,IEEE International Conference on,pp. 1-6, 2009.

[13] J. J. Haas and Y. Hu, “Secure Unified Cellular Ad Hoc Network Routing”, Global Telecommunications Conference (GlobCom), pp1-8, 2009.

[14] J. Suresh and V. Chandrasekar, “Optimal Transmission in Multihop Cellular Networks by Detecting Irrational Nodes”, International Journal of Scientific and Research Publications, vol. 3, Issue 3, March 2013

[15] K.G Paterson, “ID-based signatures from pairings on elliptic curves”, Electronic Letters, pp. 1025–1026, 2002.

[16] Mohammad Al-Shurman & Seong-Moo Yoo, Seungjin Park, “Black hole attack in mobile ad hoc networks”, Proceedings of the 42nd annual Southeast regional conference ACM-SE 42, pp. 96-97, 2004.