ISSN: 2230-9926

Available online at http://www.journalijdr.com

IJDR

International Journal of Development Research
Vol. 07, Issue, 08, pp.14260-14274, August, 2017

ORIGINAL RESEARCH ARTICLE

Open Access

SECURITY OBJECTIVES BASED KEY MANAGEMENT ALGORITHM FOR DEVICE-TO-DEVICE APPLICATIONS

***Feras Masoud, Mohammad Alchaita, and Mohammad Assora**

Computer Science Department, Syria Higher Institutes for Applied Sciences and Technology, Damascus, Syria

ARTICLE INFO

Article History:
Received 19th May, 2017
Received in revised form
25th June, 2017
Accepted 20th July, 2017
Published online 30th August, 2017

Keywords:
D2D Communication,
Free-Riding Attack,
Mikky-Sakke algorithm,
Radio Bearer.

ABSTRACT

D2D communications is the promising technology that is essential in the next generation of the mobile network. One of the basic restrictions of deploying this technique is the lack of security objectives which depends on user entities reliability and network capabilities; this issue imposes more expensive choices adopted by the network especially when user entities are out of coverage. Our work concentrated on designing the transmissions between the network and the out of coverage user entities to achieve a set of desired security requirements based on network policy applied by the SDN. The Key materials of MIKEY-SAKKE protocol are used to exchange the shared secure key, along with elliptic curve based Tate-Lichtenbaum pairing are used to achieve the security requirements. A bundle of security objectives is achieved represented by fundamental security objectives such as confidentiality, integrity and availability. The other security objectives such as the source/receiver non-repudiation, the avoidance of free riding attack and the privacy are also achieved.

****Corresponding author***

Citation: Feras Masoud, Mohammad Alchaita, and Mohammad Assora. 2017. "Security objectives based key management algorithm for device-to-device applications.", *International Journal of Development Research*, 7, (08), 14260-14274.

INTRODUCTION

The new directions of the next generation of mobile communications have many challenges, such as voluminous data, high data rate, large number of mobile stations in service, and unlimited demands with limited recourses. Another challenge is making mobile stations connected anywhere, anytime, and under any circumstances, with the new emerging applications that are used in both commercial and disaster situations (Rysavy Research, 2012). These challenges drive us to reconsider the network architecture and the new emerging technologies. The Software-defined network (SDN) architecture can help to make the network functionalities programmable. By decoupling control and data planes, we can apply the network policies in an elegant way. In addition, the network actions could be driven by events. On the other hand, the new technologies such as Device to Device D2D communications provide an effective infrastructure to enable new applications using direct communication between nearby user entities UEs.

This technique is proposed in response to 5G mobile communications requirements as illustrated in (Li, 2014) to increase the network capacity in two basic directions; the first one is by improving the network infrastructure to face the increasing demands of the consumers by adopting new technologies such as M2M Communications, IOT, and proximity services or D2D communications; the other direction is by expanding the spectrum utilization not restricted by unlicensed spectrum. It can also be used as one of the multi-tier solutions to increase the coverage area by utilizing much more frequency bands like millimeter waves due to increased path-loss associated with these suggested bands. But, the major problem that faces D2D communications is the lack of security objectives (Wang, 2015), which make user entities (UEs) vulnerable to many kinds of attacks, especially when eNodeB (eNB) becomes out of service. Security requirements such as data origin authentication, entity authentication, privacy, and other malicious behavior mitigation must be achieved to prevent the deviation from the objectives gained by these new

technologies. Furthermore, the optimization of performance could not be achieved without mitigating the possible threats, and taking positive procedures toward malicious UEs during the normal and abnormal operations. The core concept of our work can be demonstrated in many directions, the first one is to demonstrate the powerful of the idea of pre-distributing key materials to the UEs, which gives a great versatility in the process of deriving new functions to achieve many security objectives. Since the UE is a standalone entity, the D2D communications adoption may be discouraged by the unpredictability of UEs behavior, so that, the second direction of our work, is to push the devices to make the right decisions, and to make its utmost effort, in order to achieve the objectives of the network policy. Finally, since the elliptic curve and pairings calculations can be done under heavy processes, the calculations processes are simplified as much as possible. The key materials are distributed using pre-defined secure channel, which is guaranteed in LTE-A by using generic bootstrapping architecture (GBA) (3GPP, 2016) between the key management server (KMS) and UE. This will form the basic infrastructure to derive the functions and the transmissions to achieve such new security objectives. MIKEY-SAKKE algorithm (Groves, 2012) shares a secret key between two entities participating proximity services and signs the secure message. This algorithm guarantees the confidentiality of sharing these keys, message authentication, message integrity, and sender non-repudiation. Further steps can be taken by integrating SDN architecture to accommodate the security objectives. This architecture is provided with hierarchical building and many capabilities to get more flexibility, and impose the best method to achieve the security policy objectives.

This paper is organized as follows: section 2 discusses the related works, while section 3 gives mathematical preliminaries used in different parts of the paper. Section 4 presents our proposed system model while section 5 presents the proposed protocol. In Section 6 discusses the practical results achieved by the simulation, while Section 7 analyses the security objectives achieved by our protocol, in section 8 we conclude the paper and propose some future works.

Related Works

Many security aspects are addressed in (Zhang, 2015) when two user entities reside within network coverage. Privacy is handled in conditional states. More security steps are needed to prevent advanced threats such as: the selected entity may fall as a victim to malicious behavior of requesting UE by sending a beacon report to eNB while receiving a true message. The authors in (Shen, 2014) propose a secure key establishment using Diffie-Hilman key exchange with commitment scheme. They have addressed the case when the active adversary makes independent connections with victims, making them believe that they are talking to each other directly. The security management scheme for Out of Coverage UEs (OoC UEs) is proposed in (Goratti, 2014) to enable authentication of UEs, confidentiality and integrity of the messages. The pre-distributed keys with indexes are proposed to establish D2D communications by intersecting the owned index of the UE with the received index. Trade off between connectivity and overhead as a function of network related parameter is addressed. In (Sun, 2014; Xi, 2014), physical layer based relay-assisted key generation approach is proposed. The main idea is to explore some relay nodes in the vicinity of two target nodes and use the random channels associated with these relay nodes as additional random sources for secret key generation between the two target nodes. In (Sun, 2014), the mobile nodes are partitioned into disjoint coalitions. Game theory is introduced to motivate the nodes within the same coalition at the vicinity to play a rule as relays, in which every node assists other nodes to establish a secure connection and gets help from the others in return. While in (Xi, 2014), the adversary is an eavesdropper, which assumed to be passive. The channel is proposed to change slowly; the cooperative scheme proposes to keep the generated key secure from both the adversary and relay. The multiplexing gain in the key rate grows linearly with the number of relays. The authors in (Panaousis, 2014) propose a Secure Message Delivery Game (SMDG) protocol. The primary objective is to choose the most secure path to deliver a message from a sender to a destination. Energy consumption and QoS are considered by giving certain weights to the involved parameters (security, energy, QoS, etc.).

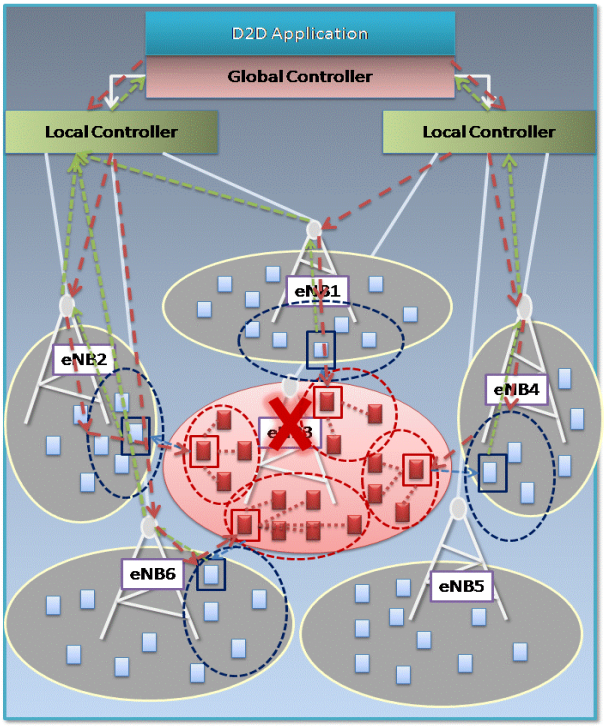

Fig 1. System Overview

Preliminaries

Definition1: Suppose that three Abelian subgroups, the following mapis: e : $\mathcal{G}_1 \times \mathcal{G}_2$ $\mathcal{G}_T$ admissible pairing if the following properties satisfied:

Bilinear:

$$e(P + P', Q) = e(P, Q).e(P', Q) \quad (1.a)$$

$$e(P, Q + Q') = e(P, Q).e(P, Q') \quad (1.b)$$

Non-degeneracy:

if $P \neq 1_{\mathbb{G}_1}$ and $Q \neq 1_{\mathbb{G}_2}$ then $e(P, Q) \neq 1_{\mathbb{G}_T}$

Symmetric:

$$e(P,Q) = e(Q,P) \quad (2)$$

Efficiency computable:

Where.

$$P, P' \in \mathcal{G}_1, Q, Q' \in \mathcal{G}_2$$

From Eq(1), we can infer that:

$$e(aP,bQ) = e(P,bQ)^a = e(aP,Q)^b = e(P,Q)^{ab} = e(bP,aQ); for\ a,b \in \quad (3)$$

The modified Tate-Lichtenbaum pairing along with the notions used in (Silverman, 2008) is defined as in (Barker, 2015):

$$t_r : E(\mathbb{F}_q)[r] \times E(\mathbb{F}_q)/rE(\mathbb{F}_q) \quad \mu_r : t_r(P,Q) = f_P(Q)^{(q-1)/r}$$

Where

$$rE(\mathbb{F}_q) = \{Q = rP : P \in E(\mathbb{F}_q)\}, \text{and } (\mathbb{F}_q)^r = \{b = a^r : a \in \mathbb{F}_q\} \text{ and } \mu_r = \{x \in \mathbb{F}_q | x^r = 1\}.$$

This pairing is considered admissible.

The practical algorithm used to compute Eq (3GPP, 2016) is Miller algorithm, with many improvements suggested by Baretto paper (Barreto, 2002) to accelerate calculations, these improvements include:

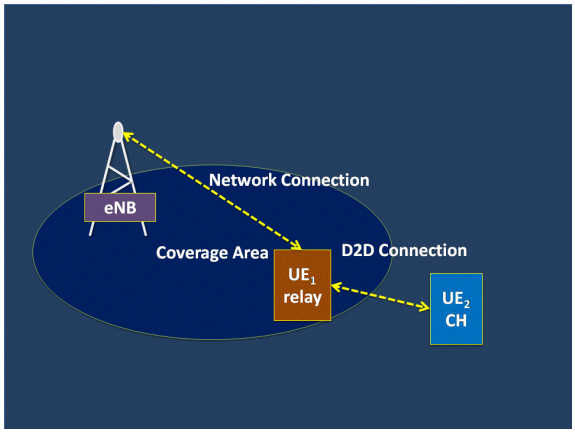

Fig 2. D2D Communications: UE-to-network relay

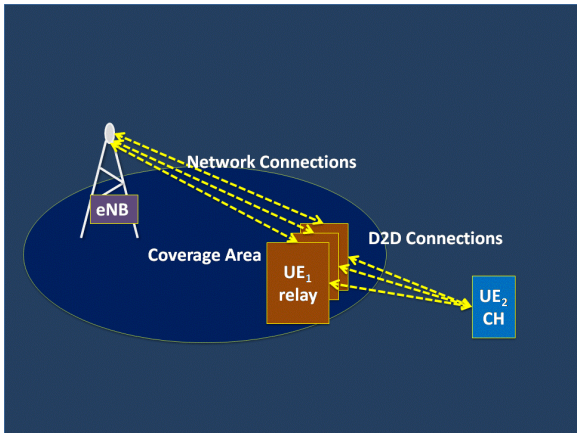

Fig 3. The possibility of using more than one of in-coverage area UEs as relays

- The points are directly inserted in calculations without using of divisors.
- Projective coordinates used to accelerate group law calculations.
- Denominator irrelevant.
- Speeding up the final power.

A special case in super-singular curves where the distortion map can be used; the distortion map used in our work is:

The extension field with embedded degree is used. A distortion map contributes a further facilitation by using a single point in calculation pairing where:

Definition2: MIKEY-SAKKE protocol (Groves, 2012) is a method of key exchange that uses Identity-based Public Key Cryptography (IDPKC) to establish a shared secret value the algorithm used to make secure connections between two or more parties by sharing the secure key, validating its correctness and signing it. The primary motivation for MIKEY-SAKKE protocol is the idea of pre-distributing key materials to achieve many security objectives, especially when the stations are out of coverage; another motivation is the low latency of real-time communication; and finally the KMS which is a trusted party of all stations within domain is used to form broad categories of security materials to face even more advanced attacks.

System Model

System overview

Suppose that we have a system as illustrated in Fig 1. In this system, the global controller (GC) has an overall overview about the network activities, and provides programmable connectivity between core network entities at the northbound interface and user plane connectivity, with QoS needed at the southbound interface. GC applies the specified policy. The local controller (LC) drives many eNBs, and combines radio access network functionalities; thus, the access network is not restricted to LTE-A network. Therefore, the transmissions to achieve certain security objectives can be applied, such as Wi MAX, Wi Fi, and W-CDMA. In addition, LC provides a hierarchical architecture of eNBs which simplifies transitions between frequency bands and resource allocations. Suppose that one of the eNBs has dropped for some reason; the GC decides to use relays at the edge of the affected area to make secure connections between LC and OoC UEs, and use MIKEY-SAKKE protocol (Groves, 2012) to share the secret keys and sign it. The key materials that allow MIKKE-SAKKE protocol () are previously provided to the UEs in the affected area by the key management server (KMS) (Groves, 2012; Groves, 2015), which is a trusted party to all stations reside within the domain. Where IDi is a short, unambiguous identifier assigned to each user. Ki is the received secret key provisioned by KMS to share a secure message of a certain length with other parties using a SAKKE algorithm (Groves, 2012). (SSKi, PVTi) pair is used to sign the secure message by the signer and validate the signed message by the verifier using Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption algorithm (ECCSI). Where SSKi is the secret part of the algorithm and PVTi is the public part (3GPP, 2016).

On the other hand, the LC is assumed to participate within KMS domain with key materials (IDeNB, KeNB, SSKeNB, PVTeNB). The secure connection between LC and OoC UE is established over a relay using D2D communication between the relay and cluster head (CH). To reduce collisions due to announces in the affected area, OoC UEs elect CHs and join to it. CHs plan the resources temporarily between the stations, and the CH is the only part that announces its presence inside the affected area as illustrated in Fig 2. UE1 is called UE-to-Network relay as the name suggested by (3GPP, 2016).

Cluster Head election and out of coverage group formation

When a node that is out of coverage needs to announce itself, it will be vulnerable to collisions with other nodes due to collisions. On the other hand, if a node is using previously dedicated band, it will not guarantee that someone on the same band listens to it. To overcome this problem and reduce the bands dedicated to such announcements, we need to control the percentage of stations that are announcing themselves and serving the other parties in the affected area by electing CHs. If a CH does not serve the other stations; the stations may elect another CH. In our proposed framework, the LEACH protocol (Mahapatra, 2015), which is used in Wireless Sensor Networks (WSN), is used to elect CHs.

Choosing CHs is done by using the following steps:

- Each node chooses a random number between 0 and 1.
- The node is chosen as CH if the chosen number is less than the threshold:

$$T(n) = \begin{cases} \dfrac{p}{1 - p\left(r \bmod \frac{1}{p}\right)} & if n \in G \\ 0 & if n \notin G \end{cases} \quad (4)$$

Where:

- p is the desired percentage of CHs.
- r is the current round.
- G The set of the nodes that have not been CH for the last $\frac{1}{p}$ round.

By this formula, we can control the desired percentage of CHs. The other nodes join the nearest CH and regulate the resources inside the affected area temporarily, by using the LEACH protocol access method. If one of the CHs does not serve the stations in its area, they can do another round to choose another CH.

Relays

In the following discussion, we want to rejoin the CH securely to the mobile network over relay. The bottleneck in the process is the relay, since it has no motivations to participate in the process due to frequency resource sharing, hardware storage, and computation loads. Moreover, it may act malicious behaviors such as:

- It may ignore the CH transmissions.
- It may impersonate other stations like eNB, if it has enough information.
- It may pretend that it cannot access the CH, and make it out of reach permanently.
- It may pretend that CH has performed wrong transmissions, so the network will apply a certain policy toward CH.

Besides that, the relay that helps CH may impose radio resource and hardware sharing, which has negative effects on the relay performance. Three steps can be taken to help relays:

- To avoid the frequency sharing, eliminate the performance degradation of the relay, and allow it to use its own band. The dropped eNB radio resources may be reused again, or dedicated D2D radio resources are allocated to establish a D2D radio bearer between LC and relay. By this way, the D2D radio bearer is used to provide OoC UE connectivity over relay.
- The required computation processes and data storage volume of D2D communications must be reduced as possible as we can.
- Distribution of the dedicated D2D communication load to the minimum limits is achieved by invoking more than one relay that is located nearby CH as illustrated in Fig 3 (this involves another task as we will see later).

By using these steps, we can make D2D communications between the relay and the CH as transparent as possible from the relay viewpoint. Choosing possible relays can be done by using evolved serving mobile location center (E-SMLC) that is located in the core network. The CHs search process by relays is not effective, since it involves many transmissions, which may cause redundant transmissions. At the same time, the CH announcement may be vulnerable to ignorance by relays. We will call the relay as UE1, and CH as UE2 for simplicity, and we will differentiate between them as needed. LC can be replaced by eNB to make sense that the radio connection is between eNB and UEs. At the beginning, we suppose some principles that allow secure connection between eNB and UE2 to achieve some security objectives:

- UE_1 must not ignore UE_2 messages; the massages must not be modified or forged by UE_1.
- UE1 cannot pretend UE2 error transmissions without evidence.
- Since UE2 is isolated from the outside world, so any connection with it must be certified by KMS to ensure source authenticity.
- When UE1 malicious behavior passes beyond a certain level, the network has the right to apply a certain policy to prevent such behaviors.

First of all, we use the statistical database figured in TABLE 1 similar to that used in (Zhang, 2015), for tracing the behavior of relays at the edge of the affected area. We send a token message to the relays. The token message is the obligation by the network on the relay; this obligation will make the relay selects the CH and never ignore its message, or modify or forge the messages. A token is sent to more than one relay. The basic condition is that relays don't know each other, and thus we can assume that relays cannot collude with each other to make CH out of service. The local controller is responsible for making decisions about true/false transmissions; the decision making rule is that:

- If some of relays admit that the transmission by the CH is false, but at least one of the relays admits that the transmission is true with evidence, then the decision is that all the relays that admit false transmission will get false transmission in their records in the statistical table, and the relays with true transmission will get true transmission.
- If the network detects that one of the relays has forged the message by CH, then it will get a false transmission in its record.
- If all relays admit false transmission by CH, then the CH is a malicious station.
- If the relays admit that no reply from a CH, then the CH is considered inaccessible.

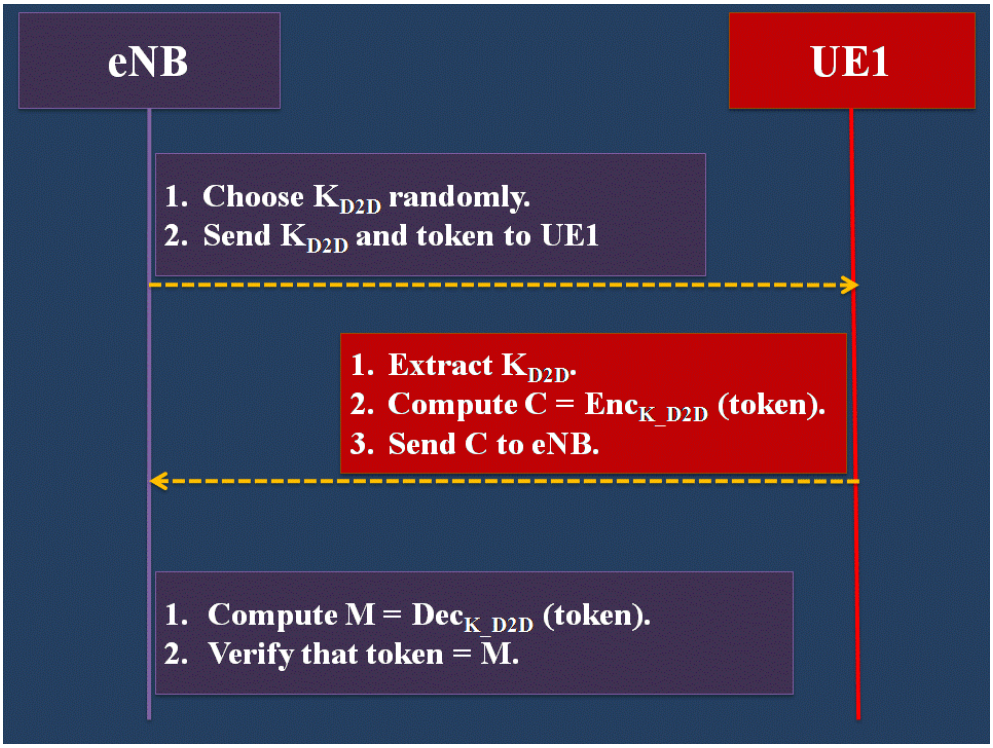

Fig 4. Transmission between eNB and Relay to establish Secure D2D Radio Bearer

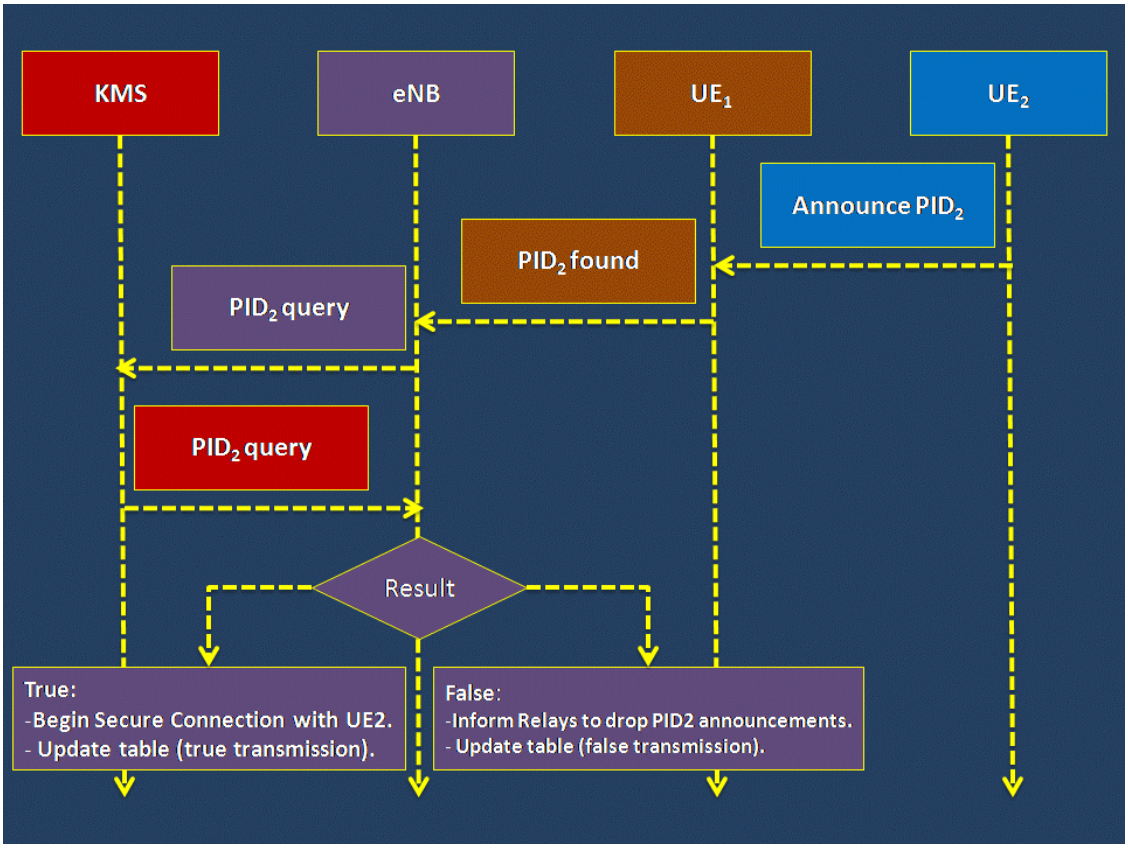

Fig 5. CH discovering stage and the processes taken by eNB

- If the wrong transmission rate of relays passes beyond a certain level, the network will apply a certain policy toward it.

Table 1 is a convenient tool as it can be used to evaluate the performance of each node, which is the authentication degree of each relay. Another benefit is to distribute the load equally between relays. More complicated decisions with invoking the game theory could be used to increase the performance of the relays, especially for nodes with low authentication degree levels; and make the relay exploits its best effort to find the CH or any UE inside the injured area.

D2D radio bearer between eNB and UE1

In this section, we demonstrate how to establish a secure D2D radio bearer between eNB and UE_1 (relay), which is different from Radio Resource Control (RRC) bearer. Non-Access-Stratum (NAS) protocol (3GPP, 2009) is still used in here, since we need the same objectives to achieve D2D radio, and the key lengths are the same.

Mutual authentication is achieved previously when UE has attached the network. In D2D radio bearer establishment, we need to deliver the secret key K_{D2D} in a secure manner. Hence, send the token message to UE_1, and confirm that K_{D2D} and the token are delivered correctly. The procedure is illustrated by Fig 4, and explained in the following:

- Find the secret key between eNB and UE_1 which called $K_{D2D.}$
- A token message must be delivered correctly to the relay.
- UE_1 encrypts the token message with K_{D2D} and returns the result to the eNB.
- The eNB verifies that the message and the key are delivered correctly.
- Mutual authentication is not needed, since it is previously preserved. The establishment is done by using RRC radio bearer.

Searching Stage

As UE_1 receives the token message, it will begin to search the UE_2 announcement. The UE_2 is prevented from announcing its ID directly, but it uses another format such as hashing its ID; PID_2 = hash (ID_2). When UE_1 captures the announcement message that contains PID_2, it will redirect the message to the eNB, which enquiries KMS to get more information about CH of UE_2. If this step is not completed properly, the eNB will inform relays to drop any announcement that contains PID_2. But, if it is completed properly, then the statistical table is updated with true transmissions for relays that found PID_2; as illustrated in Fig 5.

Joining Cluster Head to mobile network

The CH is vulnerable to many kinds of threats, since it does not have any way to identify the stations that are trying to connect with it. Furthermore, it does not guarantee that these stations are ready to provide the requirements. The CH needs to communicate securely with trusted stations that are authorized by the mobile network as relays; and communicate securely with the nearest eNB over relays.

To join the CH securely, we need:

- Secure connections with relays.
- A secure connection with the nearest eNB over relays.

Joining OoC UEs to mobile network

After the CH joins the mobile network over relays; we need to rejoin the other stations inside the affected area. Since the CH has the same token message, the same imposition and the same procedure are applied by the network. UE_1 is the station that possesses the token message. We want to deliver the token message to UE_2.

When a station is rejoined the mobile network, it will participate in the joining process to distribute the processing load. The joining message to an OoC UE, which is originated from the eNB, can be delivered either by the CH or another recently joined station.

The Proposed Protocol

In some cases like the state illustrated in the previous section; we can see that the potential threats impose more security objectives such as, entity authentication, free-riding attack prevention, and receiver non-repudiation, to deal with such threats. We introduce the concept of certificate, which allows the CH of UE_2 to validate that the eNB or the relay of UE_1 is authorized by the KMS (the trusted party to all stations within a domain) to perform this connection. On the other hand, the eNB, by getting sub-authority from the KMS to perform entity authentication, can identify the CH. Another security requirement at this stage is to get the confirm messages from UE_1 with evidences, when a correct message is sent by a CH. An additional security requirement, the eNB needs to prevent the attack, when the CH sends a true confirm message to a relay and a wrong evidence message to the eNB. This may be considered as a malicious behavior by the relay, while the CH is the malicious station.

The eNB is responsible to prevent malicious behaviors of relays, by providing them with a certificate from the KMS, and to apply network policy when a malicious behavior is detected. If we achieve this task, then we get a secure connection between the eNB and the CH over a set of unsafe stations from the CH viewpoint. Finally, the privacy requires that IDs must be preserved, so, the announcements must not involve sending IDs in clear. Two different functions of a real ID are used; one for transmission and the other for computational processes. Where, a random number from the KMS is sent each time D2D communications is needed. The traffic analysis is one of the privacy issues that can be mitigated by eliminating the reliance on one relay and making the traffic between relays and OoC UEs as transparent as possible. Before we start our proposed protocol, there are some modifications in MIKEY-SAKKE protocol to conceal the real IDs of the participating stations, these modifications as follows:

SAKKE algorithm:

Sender: The pair ($^{a;}$ $\mathcal{A}$) are sent from KMS.

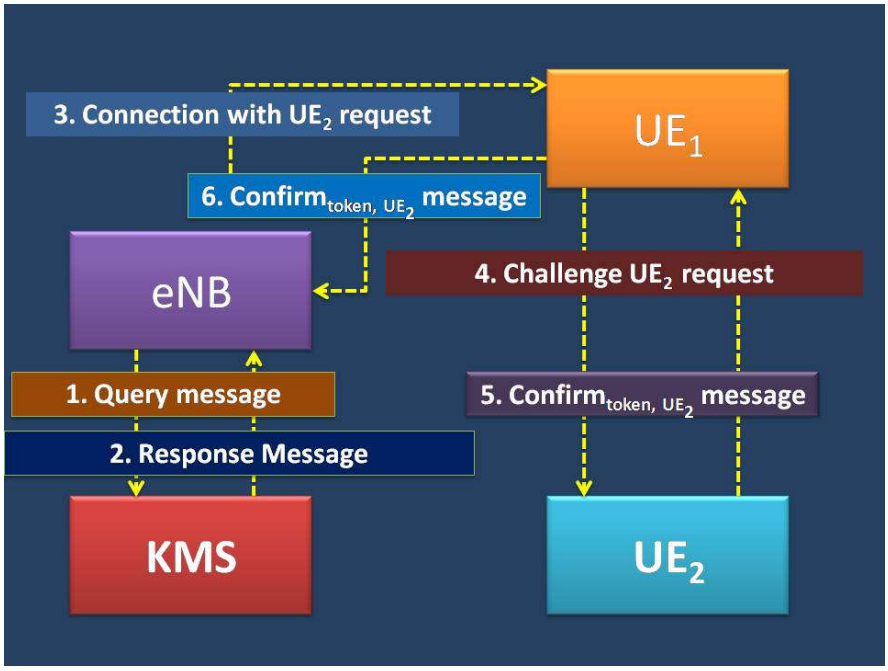

Fig 6. The message *token* exchanged between UE1 and UE2

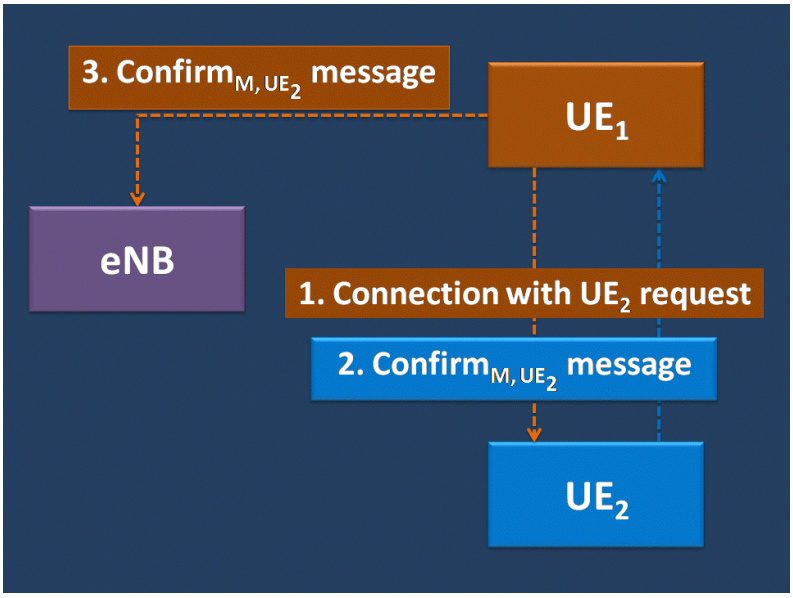

Fig 7. The message M exchanged between eNB and UE2

Relay		Relay 1	Relay 2	….	Relay n
Public Keys		PID1, PVT1	PID2, PVT2		PIDn, PVTn
	KMS	KMS1, KPAK1, Z1	KMS2, KPAK2, Z2		KMSn, KPAKn, Zn
True Transmissions (T)					
Fault Transmissions (F)					
Totla Transmissions (N = T + F)					
Percentage F / N					
S-TMSI					
C-RNTI					
Category					

Select a random integer for the SSV in the range 0 to $2^n - 1$;
Compute h_1 = HashToIntegerRange(SSV || $\mathcal{A}$, r, Hash); where $\mathcal{A} = [a.ID_{UE_2}].P$
Compute $R = [h_1](\mathcal{A} + [a].Z\_S)$ in E(F_p);
Compute the Hint, H; Compute $g^{a.h_1}$.
Compute H := SSV XOR HashToIntegerRange($g^{a.h_1}, 2^n$, Hash);
Form the Encapsulated Data (R, H), and transmit it to B;
Output SSV for use to derive key material .

Receiver

Parse the Encapsulated Data (R, H), and extract R and H;
Compute $w: = < R, K_b >$. Note that by bilinearity, $w: = g^{a.h_1}$;
Compute SSV = H XOR HashToIntegerRange(w, 2^n, Hash);
Compute h_2 = HashToIntegerRange(SSV || b, q, Hash);

Table 2. The messages used in Section 5.

Connection with UE_2 request	eNB → UE_1
Challenge UE_2 request	UE_1 → UE_2
Query message	eNB → KMS
Response message	KMS → eNB
Confirm message	UE_2 → UE_1

Table 3. The equations used in Section 5.

Equation	Calculating party
$\mathbf{S_{M,UE} = [M.SSK_{UE}].P}$	eNB
$\mathbf{\mathcal{A}_{UE_2,a} = [a.ID_{UE}].P}$	KMS
$\mathbf{C_{M,UE_1,UE_2} = < S_{M,UE_1}, K_{UE_2} >}$	KMS
$\mathbf{c_{M,UE_1,UE_2,a} = hash(C_{M,UE_1,UE_2} \parallel PVT_{UE_1} \parallel a)}$	KMS
$\mathbf{L_{UE} = hash(K_{x,UE} \parallel ID_{UE})}$	KMS, UE
$\mathbf{L_1 = hash(token \parallel L_{UE_2})}$.	eNB, UE_2
$\mathbf{V_1 = hash(token \parallel L_1)}$.	eNB
$\mathbf{L_2 = hash(M \parallel L_{UE_2})}$.	eNB, UE_2
$\mathbf{V_2 = hash(token \parallel L_2)}$.	eNB
$\mathbf{Y_{UE} = [HS_{UE}].PVT_{UE} + KPAK_{UE}}$	UE_1, UE_2, eNB, KMS
$\mathbf{Confirm_{M,UE} = hash(M \parallel L_{UE})}$	UE_2
$\mathbf{U_1 = hash(token \parallel Confirm_1)}$	UE_1
$\mathbf{U_2 = hash(token \parallel Confirm_2)}$	UE_1
$\mathbf{D_{M,UE_2,UE_1} = < [M].Y_{UE_1}, K_{UE_2} >}$	UE_2
$\mathbf{d_{M,UE_2,UE_1,a} = hash(D_{M,UE_2,UE_1} \parallel PVT_{UE_1} \parallel a)}$	UE_2

Table 4. The bit lengths of different parameters

Key Exchange Method	MIKEY-SAKKE	
HashToIntegerRange	As illustrated in RFC6508[6]	128 bits
Hashfn(str, 'SHA-256')	SHA-256 As in [15]	256 bits
n		128 bits
: ***The size of symmetric key***		
$p = (p_x, p_y)$		(1538 bits, 1537 bits)
r		258 bits
$g = g_1 + i.g_2$		(1536 bits, 1538 bits)

Table 5. Message lengths between different parties

Connection with UE_2 request	15762 bits
Challenge UE_2 request	11918 bits
Query message (From eNB to KMS)	6915 bits
Response message (From KMS to eNB)	4864 bits

Compute $TEST = [h2](\mathcal{A} + [a].Z\_S)$. If $TEST$ does not equal R, then B MUST NOT use the SSV to derive key material;
Output SSV for use to derive a key material for the application to be keyed.

ECCSI algorithm
Signer

- Choose j randomly between: $0 \rightarrow r-1$.
  $J = [j].P = (J_x, J_y).J_x \rightarrow h.$ Calculate HS:
  $String = P \parallel KPAK \parallel PID_a \parallel PVT.$
  $HS = HashToIntegerRange(String, r, hash).$
  Calculate HE: $String = HS \,||\, h \,||\, M.$
  $HE = HashToIntegerRange(String, r, hash).$ Verify that $HE + h.SSK \neq 0 \,(\mathrm{mod}\, r).$ otherwise go to step 2.
- $s = (HE + h.SSK)^{-1}.j \,(\mathrm{mod} r)$.
- $signature = (PID_a \parallel h \parallel s \parallel PVT)$.
- A sends the signature message to B.Verifier:

Validate that PVT is on EC. Calculate HS. Calculate HE.
$CalculateY = [s].(HE.P + [h].Y) = [SSK].G.$
$J = [s].([HE].P + [h].Y)$ Verify that $J_x = h \bmod r.$

Thus, the real IDs of the sender and receiver is concealed from each other. Suppose that, the eNB wants to send a shared secret key (M) to the CH, to secure the messages between the eNB and the CH (the key is derived as in NAS protocol). MIKEY-SAKKE algorithm (Groves, 2012) is invoked to share the secret message and sign it. The message of the form: mikey-sakke(eNB, M) means that the eNB sends a message M to the CH with a secure message:

$sec_{msg} = R_{(eNB,S)} \parallel H_{eNB}$ (Xi, 2014); and a signature:

$signature = h_{eNB} \parallel s_{eNB} \parallel PVT_{eNB}$ (Groves, 2012). Sending a message from the eNB to the CH of UE_2 means

that the KMS authorizes the eNB to send the message M, and UE_2 can validate that, so the message is considered secure. As a result, it is connected securely with mobile network via the relay of UE_1. We notice that the procedure involves exchanging two secret messages with UE_2.

The first one for exchanging a token message, which confirms that UE_2 is accessible and the eNB guarantees that relays work properly. The importance of exchanging the token message is that when the relay is moving away from the affected area, while another station is moving close to this area, the eNB immediately establishes D2D bearer with the new station, by exchanging token message with it, and sending a message to UE_2. This will make the access to UE_2 as transparent as possible. Even if the token message is vulnerable to disclosure, this is worthless without authorization from the eNB and the KMS. The second message is exchanging the M message between the eNB and UE_2. This message involves the basic key materials to extract further keys just like NAS protocol; it is designed to be of the same length (128 bits). The proposed protocol has the following steps:

- eNB sends a query message to the KMS to authorize its secure message (M) sent by eNB and (token) message sent by relay as illustrated in Fig 6; therefore it needs to send $S_{M,eNB}, S_{M,UE_1}$; the table of equations used is illustrated in TABLE 3.
- KMS receives the query, chooses a randomly; and calculates the certificates $c_{M,UE_2,eNB,a}, c_{token,UE_1,UE_2,a}$ and L_{UE_2}. The random number a is used in combination with real ID; therefore the real ID is concealed during calculations, whereas PID is used to announce the presence of the station. KMS returns the certificates along with L_{UE_2} back to eNB as a response to the query message. Note that L_{UE_2} is used as an entity authentication material that is only calculated by KMS and UE_2; thus L_{UE_2} represents a sub-authorization for eNB by KMS to ensure the entity authentication of UE_2
- eNB calculates L_1, L_2, V_1, V_2 derived from L_{UE_2}; and sends $\text{Connection with } UE_2 \text{ request}$ message to UE_1; this message includes V_1, V_2 which is used as a hint for the relay to verify the correctness of the Confirm message sent by UE_2; Note that V_1, V_2 contain a part known by UE_1 which is $token$ message and the other parts are L_1, L_2 obtained from the Confirm message sent by UE_2; by this way UE_2 can verify the correctness of the Confirm message without falling as a victim to the malicious behavior of UE_2; on the other hand, when the relay reveals the values of L_1, L_2 this is considered as an evidence to the eNB that the relay is really connected with UE_2. The message forms are illustrated in TABLE 2.
- UE_1 sends $\text{Challenge } UE_2 \text{ request}$; that contains $mikey - sakke(token, UE_1)$ and certified by KMS; the importance of this step is to achieve the benefits of MIKEY-SAKKE protocol illustrated in the previous section, another benefit is by exchanging $token$ message with UE_2 with completion of the whole procedure, the same network policy is applied on UE_2 since it is considered securely connected.
- UE_2 extracts the secure message; verifies its correctness, validates the signature and the certificate, and then calculates $Confirm_{token,UE_2}$ message then sends it back to UE_1. Note that calculated $Confirm_{token,UE_2}$ message must
- be exactly the same as L_1 message to continue the procedure.
- UE_1 verifies the correctness of $Confirm_{token,UE_2}$ and sends it back to eNB. This is considered as evidence that UE_2 is accessible if this message is correctly received by eNB. Fig.6 shows the procedure to exchange $token$ message between UE_1 and UE_2.
- UE_1 delivers $\text{Connection with } UE_2 \text{ request}$ to UE_2, the same steps 5, 6 followed to extract the secure message M, verify its correctness, validate the signature and rhe certificate, and send $Confirm_{M,UE_2}$. The secured shared message M is further used to derive further key materials to secure message exchanged between eNB and UE_2. The procedure is illustrated in Fig 7.

RESULTS ANALYSIS

To make the protocol compatible with the NAS protocol used in LTE-A network; in such case, the shared secure message length in the simulation is 128 bits, to make the security level compatible with AES-128 as demonstrated in (18). The lengths of different parameters are illustrated in TABLE 4; while TABLE 5 illustrates the lengths of the different messages used. The elliptic curve used is supersingular which has the formula given by:

$$y^2 - x^3 - ax \tag{5}$$

The elliptic curve is defined over finite field $\mathbb{F}_p$ where $p \bmod 4 = 3$. The extension field $\mathbb{F}_{p^2} \cong \mathbb{F}_p[i]$ with i such that $i^2 + 1 = 0$. In such case, the pairing calculation represented by two dimensional vector space, although the bit length in each dimension is slightly bigger, but the gain is more simplification in operations execution.

To achieve the desired security level compatible secure shared key of length 128 bits, we choose the cyclic subgroup order of the point P greater than 256 bits (Groves, 2012) (258 bits in our case). By this way, we have taken all security requirements to achieve the security level compatible with AES-128.

Security Analysis

MIKEY-SAKKE algorithm achieves many security objectives:

Table 1. Key Materials of Relay station

Station	Relay
ID	relay@yahoo.com
PID	E / 0 LK]o ?W : 8'
K	19753071594220456633238536851806811510229606273876106371640622276633728183783970935052665591076770751361451266595335233813806290003417111214271713437496815501693128188729290038144190187856256380412651809307247611364870985618432776812083771630808659096851032565982428028748767333143543647649064661159733532649217500993257976086464822465436799426171368072303625874642032823994386027470488066514771173220907431877415561391580647402655820686699819662948064222495693064996373916168692124540907120673316924866073926273949875259035242309389721457141818252534874322437619118150974733687209107085202306514413234908192159134006598246723086537838698033397477826161996839081954197688250544225505776727908376157256986059126234675340548515216918678176398919560568055146353659889631755606364454782898838463326616577551384778693172900542266045150642069702466960078372408477257630591554730334129254078311460264815901275492277799925556928161295
PVT	69243132936426841498145189297678961079779929269980267309601824021644482298123855777349046369548497475754746198023888224940738405567962754733073219166508322388089931268464613726228425065098542704661862254090807163432322876594115427898925136454813157071687517444920725374352241056384626455532344885516610042310688193751236241605297706567837943203178187111338094394248790334188555829388478730114304784991032776636890594041313815348568553555664639311133205966626354885796326921711243419195943013409823854793671678902170432637964592602119828697914396501614833247639326959988183723036416041211816468041522512396182604211304551850364294931011625385330821263238252813472152830847263896513837327695192402728764829530000731045471735605017146518809521898065764079865494816416360332290122818208796695947988063240736727328217414790945809553897956947087738627149638757004647520402035494563201831972486309004627979672843459403901570657852
SSK	3057914948861139198903586271117237653396718625814381856461793919818109945380 22

Table 2. Key Materials of eNB

Station	eNB
ID	eNB@gmail.com
PID	~I 4. %I& q Y
K	219661106972165451964768744762701079610419140045874567653385133974272846540308836421594100534906271199411996354194371343411543866239911006926704915263102596387643018663144739532013073097772006870298974869830852685407782803243068687969054011039628662999930890444390485931389917672422370920722896438664311944409771449252254024845286556398074174191177508968256788426530114828776902820251536371663150280979654336291908762726925746776404061445175654389905527699927973080984071482231212804132052514389122310025461446557709023924661089853295213250066690077378328825460231604763082360231069524667663053955292609805961494112196339114757917131930756244936483926739752267466140558775551646429158703193734315027570996293394426053059279129212452315054851659620795356672364745244319325037749581326878124742589260060846976396525550604390429726280886132877062697889970220727879890423753910810342041618626468764895266064019143555900815406530
PVT	79427048853106295484166310837275316866888429000139958439305542720958853028409297410539330254804941092767207211535839608142094914555611537738696426719926040494500904294283571246008186025912112717074245678018398565801700887955575205784437664092691423364354968316560505293112397965101087116150061174753165936099424550038320672707963530327851289631108175745376055525965883421985439877196982981780817375779198010427259948326130062609685060599424208179106249758173785371116188934535317038043243948869689696251379198358353575889401841213883964920622333870059921688160018723435311385060876637081812512774171924501375573052979032627076143709157994704241886681989663786831031343975412064666036949083045505294986718112379651052311121682322238219641928581075542953960613717242507046333271059446953564112270337909840522081590851548216358846467463231087343202775727713725444225403423058048848114761269168415979470684326745904569267213793465484292016173180909810366066959431036131908642251104385808766735584192783 44

Table 3. Key Materials of CH

Station	Cluster Head
ID	station_2@hotmail.com
PID	%p@ % kQ -' X};B mrBS
K	730897926500306351983930739639412708319545814671769129303894294302470259041155968784244958704520460576206390647576733052288511556992662636726631792351298579209440789000014554819668899177046348613068071042443866713650248396114325693812029793228086741241989257317110427323265293902063828339056774304826080336619982629889647409464879513729439177375749867172946684983970394202391902024833110054146275911918111898493369165407940243830805772927441550206988786497759428975656262974344056927850935017864282350095814336224236827255727827977642871838071485758967339775350235892814601506038923960929133685680443900989777502271740399317222384080957646619733556586202924891615960580049659969514636228113533536834553664039377632318790376942382362308882565690697379151741191111985596314443124249322919019156231099516387952912362708096412074758725414100918450425508012054237937209075732756144109560271718135179038019046333640252385974648228535756262974344056927850935017864282350095814336224236827255727827977642871838071485758967339775350235892814601506038923960929133685680443900989777502271740399317222384080957646619733556586202924891615960580049659969514636228113533536834553664039377632318790376942382362308882565690697379151741191111985596314443124249322919019156231099516387952912362708096412074758725414100918450425508012054237937209075732756144109560271718135179038019046333640252385974648228535
PVT	554585629106253440884523976803992100982758114185744704974387616228073680267416990738281510479817330611440538968084253042851695299924851473086289288766122923253829358789733804288537657623034216842804589478733618628466291828847888056508785300011055014550943748285230619797333625394296221720175498164759739401454727593897743520730629276062592925412947599795500116425781366634966850152306172702063540672542681862387650989279707247053493185943694351611540689404857792455500116425781366634966850152306172702063540672542681862387650989279707247053493185943694351611540689404857792455500116425781366634966850152306172702063540672542681862387650989279707247053493185943694351611540689404857792
SSK	1296362212958858520719544807719031624878699688325623061748252506061293145317 6

Table 4. Public and Private key of KMS

KMS Domain	
Public	
$\boldsymbol{Z}$	297450155732977237802736452325117478229089430690924984374500921158300414656515872068236444922235263880312472051061627141810930166626517714090763752527589022599765830363248781146842242142846412178575770858823125944904926291015416734100944652247414856251120365686766708490605820393515939373387652176375346704866002545734419941074027655260989766417983066954132601227593790325536601180975712298662862547583928342538888302030580055957660725282782202137490071063863976380311045481649875434638346469156432284226894758571878184077944610519334031810149568006247960761754194086682295064581685378280026736504480525099325681433390943775611622012107256622473326181883642005948771682615729634232661013731546410849714396908372428238711983155949040826803858390838787628874085062399389656300430238120990972542189064423898027829602608412926439915717945629428348769817360907186597453814738336897074949403651445653336934430367478597266596061853
$\boldsymbol{KPAK}$	190959027829759155436765967219894338913922954676390200333149085009042549169264756577571259745826804371305446799930450761314296454070621756762119823505619084979489631840252462346768790325323134820552032031783516075336659137112984866614223181374830305496412115555127942903003855370750860313385456438698627437394473659305595857580055542254861689518022432557852856090016471503332270032381512175823582380594934606564131503911581151980818231544337733815300503607892879375128347783312152340381212748692279182325061975495349812219285060154851493811751527972950773795343099711613685010255813507009107444928126196279342614511465312301740383338431397890324401506180481505283411061911290975302180208622433319020049293653362146838349707627019076253948883392954073982649082173949923189050703829235482659893188962507836116455345119049237608171318133513818026281058865349112426640689268577248396142771280541801036480216378350443688421702102799571
Private	
$\boldsymbol{z}$	737891135804302038864557666217371318132304841626567203567021242761971
$\boldsymbol{KSAK}$	249142422180907352900964535551047639915047461166942395005609737726425814020683

Table 5. Set of equations used in Simulation

Some equations used in simulation	
	KMS key materials
$\boldsymbol{KSAK}$ is chosen randomly	$KPAK = [KSAK].P$
$\boldsymbol{z}$ is chosen randomly	$Z = [z].P$
	ECCSI for the stations within domain
$\boldsymbol{v}$ is chosen randomly	$SSK = [(HS.v + KSAK)] \, mod \, (r)$
	$PVT = [v].P$
	$HS = Has \;\; ToIntegerRange \, (P \parallel KPAK \parallel PID \parallel PVT, r, Has \;)$
$\boldsymbol{j}$ is chosen randomly	$J = [j].P$
	$= J(x)$
M is the message to be signed	$HE = Has \;\; ToIntegerRange \, (HS \parallel \quad \parallel M, r, Has \;)$
	$Y = [HS].PVT + KPAK$
	$s = [(HE. \quad + SSK)^{-1} \, .j].mod \, (r)$
signature	
	SAKKE to share the secure key
KMS operation:	$\mathcal{A} = [a \, .ID].P$
$\boldsymbol{Choose\ a\ randomly}$	
	$_1 = Has \;\; ToIntegerRange(SSV \parallel A, r, Has \;)$
	$R = [\ _1][\mathcal{A} + a.Z]$
SSV is a secure shared value (the message M)	$H = SSV \oplus Has \;\; ToIntegerRange(g^{a.h_1}, 2^n, Has \;)$
	$w = < R, K >$
	$S_{M,Station} = [M.SSK_{Station}].P$
	$C_{M,Station} = < S_{M,Station}, K >$

Table 6. Security Sestem Parameters in Simulation

Security parameters used (Comparable with AES-128)		
Key Exchange Method	MIKEY-SAKKE	
HashToIntegerRange	As illustrated in RFC6508[6]	128 bits
Hashfn(str, 'SHA-256')	SHA-256 As in [15]	256 bits
$\boldsymbol{n : The\ size\ of\ symmetric\ key}$		128 bits
$\boldsymbol{p = (p_x, p_y)}$		(1538 bits, 1537 bits)
$\boldsymbol{r}$		258 bits
$\boldsymbol{g = g_1 + i.g_2}$		(1536, 1538)

Table 7. Messages lengths used in Simulation

Message lengths between different parties	
Connection with $\boldsymbol{UE_2}$ request	15762 bits
Challenge $\boldsymbol{UE_2}$ request	11918 bits
Query message (From eNB to KMS)	6915 bits
Response message (From KMS to eNB)	4864 bits
Confirm messages ($\boldsymbol{UE_2}$ to KMS)	512 bits
Mikey-sakke(M, UE)	7944 bits

Table 8. Elliptic Curve Identity Card

Elliptic Curve Parameters	
Type	Supersingular curve
Equation	$y^2 = x^3 \quad 3x\ (mod\ p) \qquad w\ \ ere\ p\ mod\ 4 = 3$
Distortion Map	$i^2 + 1 = 0$
Extension field	$F_p{}^2 = F_p(i); w\ \ ere\ i^2 + 1 = 0$
$\boldsymbol{p}$	799048157761676804698695207091974398500030087385732551402239841535085 820550121359151065572936549806341271461360702570643358085082435803004 000786240664715289966306448269334415672010790609529415722860908520259 443421832791244363955500839779181392232017080172052707138925548148308 220280711404563608362984355493619680602187369705888600568581280343457 512060066112886953313930015159364068424486378355884938693574956677513 47924442322987192030561765252614048966389340705 43
$\boldsymbol{r : where : r \mid (p + 1)}$	387686147224663765133129979655334395983602681863975442378889907832709 881240927
$\boldsymbol{P}$	528097744603049598994712708335738015121310823385843770420836965793887 892354174849663224856518515012200991967159172636467423104377739155885 028285875023009863572100777384971569944351878791328808842032892761349 622342510823440197242729514795827186984730484373974982268224031372845 977376984505506206152520362718758922708296265496329330808362736810850 178382691922320112785199876326777320166442422399477866789130984159 73 098550733101477165884211759503101335476769600 5209 366086023055917599287265169651294269737911627675181389121740755241513 596830056589105396857062444240646632467231935218150209486820396548712 458294317147037370929971325060376629510773862275667664165408837959950 413430457588320976825048258774659380319505186184614320210808175019785 263596359623144374084627317007497718207052268641845733671920570267559 085181014286619487155754254979539308395193223612795915269936087991734 153985817513961914016991861113523499037994010 2014
$\boldsymbol{g = < P, P > \in F_p{}^2}$	232896244957774210815696141879266345652356603481469350776252073991643 357811962854424697546842946754725874126200238809783052286106996893 55 363439619756955627572386869581187513059643543589497374286130693851807 489775799997555726717982725372334845537729459101066454812102604055802 320160848087556113636216756647980347338200272318904789768265211200465 253984187640740556192340430692543617992299899696132533443622250864234 942225766160222111555425217319203050707490485959 7 580101282845028965822126664356656438434318523124005744719697140164094 523493451960742646856838576877095379535372744609619862025071200780917 964841523499685591768556774675511918581230072181774836795553736985917 243736900958723502947872413861526278645711491196815445302337118412450 019624978893873595878130936664663205613533616379071626967051804066085 433030968636122480547160843066536353576396506211685983375958806004708 768532535829222936779096616802540406572904728473 9
Pairing model	Tate-Lichtenbaum pairing / Baretto's trick is used.
Coordinates	Projective coordinates / Affine coordinates

- Confidentiality
- Integrity
- Source authentication for achieving D2D communications and residing within the accepted KMS domain.

Entity authentication is achieved by using the certificate that allows the OoC UE to validate the relay and the eNB by ensuring that the received messages (token, M) are authorized by a KMS which is a trusted party within the domain. The confirmed message guarantees that the intended receiver has extracted the message correctly; therefore, the secure connection has been made by the authorized entity and mutual authentication achieved. Receiver non-repudiation: When the relay obtains a true Confirm message, it is considered an evidence that the OoC UE has received the message correctly.

Table 9. The results of Proposed Transmission by using the Simulation

Parameters obtained by using the proposed algorithm	
KMS Operation	
a	1147334347446287566433880643380076042579465413446811332910556019065227481305 12
$\mathcal{A}$	2090908573752173653537544235561115975965656863812891893755543815314814877599577645884474017154685180841 1882420023391542543187659300080134314326945754146577488120216874921458609588930707124219224112954917813 1389266508668334436467589994284954079623184084712033017046942631192659595589668827810044392967486774828 4838827127249339249906061113238627596960213972085290137074636097003805337962692800993648062599211090583 7739932472413657582038570620350520518003029031999 22 2041401470051706716397244505276705289796490712991199404316197210588408965200456701685926748667000287957 2341291545650694890249258853625076555467185639426163959239778168566314910095112874715384068242928765340 9546649258033271686006968081302299290033491033570418787182104287163314299055899395966736946595265268347 1211010376054437443891761497491076847899978042731730580902221840318881086635884921288017112196203020034 1523500935158804277538629638916210423550722851151 01
$S_{M,eNB}$	7203955058045414176963306790480540385200026482810655923136111210163371313714549701861421889818195545118 4542871636820699920720222347274167110654764983364759590104228724324208651687479895545836876227031685605 4050979871134175322476191807228784570872470764237860402668514837258594053992090035350131379604098379888 6291330695394234434802972852323974747008117154576482639903434623766701983699364721953380474815893632174 2657913437371718983134920825035865905806482618164 61 7414968048992111363756324172759576508979740223828323558713650977200818983138030781684728211545426815917 3610440756874640331172975437144982290100298019706528819384704449414314771973265629985406498166401932693 8221273239889286326363149809591464304757654822417937504954754896445697792347271554672179349442936489980 2144121129610395126591041474749696494510793827079591312121464523257732067958915675236113579680011269580 1069953091792682534795518235006835996115024038800 31
S_{token,UE_1}	4964163854527727830756212816240200380483121266076137725352192658946494056013819839409982254935881308614 9759858732300961472709701859453410371725131914691713482065751961800619233619698797572808599888553652175 5974565038601776759611343711299211037092535267279177941178619285324241361783890473081658500029607950913 1092978440514547166086633912914544208824317840997156878900312468562427182927845550207202033578170568166 5516860326764890483167350106449693843684160541705 21 7010315228093839814694479167316972457610203690437831765364707158886992588075135381614567331772491885661 1736577268046030302944649675948320109377755861805074303333760844708120158804540194792639541656383034999 0186383913248672713805349940944329398328409019754118796567722552201159848868816697922063098259299387 52 2046739205849746602450312145040593592490773375188647535088556812297053801006745077437963964527544639497 0811163143032344234899942902791961921378799404363
$C_{M,eNB}$	3079488480277200623822018841159996425832734120018326164576722546055366679900400134690509023184937154452 3441367037149279176249874527487659794587546042719544523879569081376057581050031278631884842276401237 87 1747588481830114714090953441673490300439132673528177268367021757472550367212954230560282524711357382993 9601948789417865154274231025205800636467646579789070664645346628604758772802768046784025502415685745378 3156970313271166662826151684029550232456109008438 94 6112418174847178724132819628755632297107151650871473224775823536818057096558122869140146979101728837561 0237191986873842617216662298607803360037261790114190044070124263994398629720973738928050713931381 4024 4959039395256841684719223425129686228219862750167317013654595635290459878235104450796523128786548223865 2297168957590278190428861859119488192358775924324403821213923900643322746872090600390986846041175764910 5994972290872526271242876892124166514453149326970 12
C_{token,UE_1}	2849590443357666713866343558164832916095221565589021211964126178419989434020205973019616893212747212269 1775038303259585056293395360923075120294686031279491967091534258372133253287361419937287540071021128592 0870619120134193967072743558870301782278815742899840205313249342194181188355546501848900241098904079288 4541455170068062209894891662594641500657659620698322421041826965556715568613382789199578600952439118497 1707816424492731544555492440757050611634538556573 5 4368657311915671579454502589550621222573190368340132480705021323644576299824827564500582332467968700933 3570181305725610688307357033175330581407855916368233557845504586432467781814463475488689751179137533310 4195044515672141245139446935620575558671481808942696778180069346542174932682183123279683390412574302349 5017115977478168175668242702549925801828122436795058205771139912396691617662236755323322326576938635266 8104099071748384107941800558886864251646754101530 20
$c_{M,eNB}$	9 TL o] ;rN 9Ngv
c_{token,UE_1}	% ! oL r = x g g :g^
L	t WR [, u^ v f
eNB Operatation	
L_1	z 6) g <F ,v L S
V_1	=i 9, 6Z 4V7}{kN) >
L_2	uA m |i kNW= b0@ na
V_2	5d S {W `N> b ` qy!1
UE_2 Operation	
D_{token}	2849590443357666713866343558164832916095221565589021211964126178419989434020205973019616893212747212269 1775038303259585056293395360923075120294686031279491967091534258372133253287361419937287540071021128592 0870619120134193967072743558870301782278815742899840205313249342194181188355546501848900241098904079288 4541455170068062209894891662594641500657659620698322421041826965556715568613382789199578600952439118497 1707816424492731544555492440757050611634538556573 5 4368657311915671579454502589550621222573190368340132480705021323644576299824827564500582332467968700933 3570181305725610688307357033175330581407855916368233557845504586432467781814463475488689751179137533310 4195044515672141245139446935620575558671481808942696778180069346542174932682183123279683390412574302349 5017115977478168175668242702549925801828122436795058205771139912396691617662236755323322326576938635266 8104099071748384107941800558886864251646754101530 20

Continue…….

$c_{M,eNB}$	9 TL o] ;rN 9Ngv
c_{token,UE_1}	% ! oL r = x g g :g^
L	t WR [, u^ v f
	eNB Operatation
L_1	z 6) g <F ,v L S
V_1	=i 9, 6Z 4V7}{kN) >
L_2	uA m |i kNW= b0@ na
V_2	5d S {W `N> b ` qy!1
	UE_2 Operation
D_{token}	284959044335766671386634355816483291609522156558902121196412617841998943402020597301961689321274721 226917750383032595850562933953609230751202946860312794919670915342583721332532873614199372875400710 211285920870619120134193967072743558870301782278815742899840205313249342194181188355546501848900241 098904079288454145517006806220989489166259464150065765962069832242104182696555671556861338278919957 860095243911849717078164244927315445554924407570506116345385565735 436865731191567157945450258955062122257319036834013248070502132364457629982482756450058233246796870 093335701813057256106883073570331753305814078559163682335578455045864324677818144634754886897511791 375333104195044515672141245139446935620575558671481808942696778180069346542174932682183123279683390 412574302349501711597747816817566824270254992580182812243679505820577113991239669161766223675532332 232657693863526681040990717483841079418005588868642516467541015302 0
D_M	307948848027720062382201884115999642583273412001832616457672254605536667990040013469050902318493715 445234413670371492791762498745274876595794587546042719544523879569081376057581050031278631884842276 401237871747588481830114714090953441673490300439132673528177268367021757472550367212954230560282524 711357382993960194878941786515427423102520580063646764657978907066464534662860475877280276804678402 550241568574537831569703132711666628261516840295502324561090084389 4 611241817484717872413281962875563229710715165087147322477582353681805709655812286914014697910172883 756102371919868673842617216662298607803360037261790114190044070124263399439862972097373892805071393 138140244959039395256841684719223425129686228219862750167317013654595635290459878235104450796523128 786548223865229716895759027819042886185911948819235877592432440382121392390064332274687209060039098 684604117576491059949722908725262712428768921241665144531493269701 2
$d_{M,eNB}$	9 TL o] ;rN 9Ngv
d_{token,UE_1}	% ! oL r = x g g :g^
$Confirm_1$	z 6) g <F ,v L S
$Confirm_2$	uA m |i kNW= b0@ na
	UE_1 Operation
U_1	=i 9, 6Z 4V7}{kN) >
U_2	5d S {W `N> b ` qy!1
$token$	308896546772799995306343897777196609647
M	28771360277421175199971928038261711942 8

The sent message by the relay or the received Confirm message cannot be forged or impersonated by the relay since it is subjected to the game theory applied by the network; hence, the risk of losing service should a malicious behavior pass beyond a certain level. On the other hand, a malicious behavior of the OoC UEs can be avoided by sending the hint messages (V_1, V_2) to the relays. Avoidance of free riding attack: The steps that are taken by the network to mitigate the malicious behavior of relays along with the game theory, based on decision making, will prompt the relays to make the right decision by responding to the announcements issued by the OoC relays. Privacy: The real IDs of the stations participating in the procedure are concealed from each other.

The process of decoupling the real IDs used in calculations, from the transmitted IDs used in announcements, will achieve several objectives: The network and the stations deal with real entities and not impersonations. Any party trying to use the announcement ID without the ability to produce true Confirm messages will be considered a malicious behavior and will be captured by the network which applies the policy concerning malicious stations. Furthermore, traffic analysis is impossible since traffic to the receiver is delivered over multiple relays. The assumption that the relays do not collude with each other is important and reasonable since this is one of the game theory requirements. Should the two relays try to make s D2D connection, they need authorization from the network and the connection will be temporarily aborted by the network until the joining OoC UEs is completed.

Availability: By using mini-cloud of relays isolated from each other at the periphery of the affected area, the availability requirements can be achieved and the bands used by the affected eNB can be redistributed over these mini-clouds to achieve the required SLA. A potential performance degradation does exist due to the relays' degree of reliability. The transmissions between the relays and the OoC UEs are as transparent as possible due to the possibility of moving one of the relays away from the affected area. Should another in-coverage station move close to this area, the network can immediately send a token message and an authorization to this station to work as a relay. The availability and connectivity have been discussed in (Zhang, 2015) and (Goratti, 2014); however, this study needs further consideration and scrutiny to explore the issues related to the authentication degree of the relays, as inferred by the statistical table and from the viewpoint of traffic engineering in order to achieve the required SLA at extreme states.

Conclusion and Future Works

D2D radio bearer has been introduced to reduce radio sharing and performance degradation with relays, this bearer may be the downlink connection of dropped eNB, unlicensed bands, or any other expanded spectrum utilities available by the network, this process has the mean of re-identification of radio resources allocated for each OoC UEs, The QoS is guaranteed by the minimum SLA in abnormal circumstances dedicated by the network policy. This framework employs more than one relay to distribute the hardware load, storage capacity, and heavy processing.

Moreover, it conceals the relays' IDs and does not depend on one party. The statistical table is introduced for tracing relays behaviors. The decision that is taken by the LC is important to improve relays reliability. The game theory can be used in relays to build the decision rules that are based on relays reliabilities. By using certificates with MIKEY-SAKKE protocol to help CH communicating with trusted stations, we can share keys securely, provide message origin authentication, message integrity, and source non-repudiation. Moreover, the framework provides entity authentication for OoC UEs, in addition to receiver non-repudiation. The sub-authority technique allows the KMS, which has a full authorization capability, to authorize the eNB or a trusted station to perform a number of security services such as entity authentication. Further steps can be taken to authorize the eNB to certificate its message without communicating with the KMS. The framework conceals the IDs of participating stations to maintain the stations privacy, since we do not have any idea about the attackers' capabilities. Therefore, this will mitigate unpredictable malicious behaviors of some parties. As we have seen; the functions and parameters that are used for sending and computing are different, which means that the only entity that can send and compute the transmissions properly is the station that has the real identity. Through our work; we have introduced a realistic scenario that may 5G mobile network encounter. This scenario can be generalized with the same technique, and the same security objectives to be a framework for D2D communications, when user entities are out of coverage.

REFERENCES

Rysavy Research, 2015. "Beyond LTE: Enabling the Mobile Broadband Explosion", *4G Americas*, White Paper, Aug.

Li, Q. et al. 2014. "5G Network Capacity/ Key Elements and Technologies", IEEE Vechular Technology Magazine, vol. 9, no. 1, Jan. pp. 71-78.

Wang, M. and Yan, Z. 2015. "Security in D2D Communications: A Review", IEEE Trustcom/BigDataSE/ISPA, vol. 1, Aug. 2015, pp. 1199-1204.

3GPP, 2016. "Study on Security issues to support Proximity Services (ProSe)", 3rd Generation Partnership Project (3GPP), TR. 33.833, Release 13, Feb, pp. 1-231.

Groves, M. 2012. "MIKEY-SAKKE: Sakai-Kasahara Key Encryption in Multimedia Internet KEYing (MIKEY)," RFC Editor, California, RFC 6509, Feb. pp. 1-21.

Zhang, A. et al. 2015. "SeDS: Secure Data Sharing Strategy for D2D Communication in LTE-Advanced Networks," IEEE Transactions on Vehicular Technology, vol. 65, no. 4, Mar., pp. 2659-2672.

Shen, W. et al. 2014. "Secure Key Establishment for Device-to-Device Communications", IEEE Global Communications Conference (GLOBECOM), Austin, TX, USA, Dec. 8-12, pp. 336-340.

Goratti, L. et al. 2014. "Connectivity and Security in a Device to Device Communication Protocol for Public Safety Applications", Wireless Communications Systems (ISWCS), Barcelona, Spain, Aug. 26-29, , pp. 548-552.

Sun, J. et al. 2014. "SYNERGY; A Game-Theoretical Approach for Cooperative Key Generation in Wireless Networks", IEEE INFOCOM- IEEE Conference on Computer Communications, Toronto, ON, Canada, Apr. 27-May. 2, , pp. 997-1005.

Xi, et al. 2014. "KEEP: Fast Secret Key Extraction Protocol for D2D Communication", IEEE International Symposium of Quality of Service (IWQoS), Hong Kong, China, May. 26-27, pp. 350-259.

Panaousis, E. et al. 2014. "Secure Message Delivery Games for Device-to-Device Communications", Springer International Publishing. 5th International Conference, GameSec, Los Angeles, CA, USA, US, Nov.6-7, 2014, Springer, Nov.6-7, 2014, pp. 997-1005.

Washington, L. C. 2008. Elliptic Curves Number Theory and Cryptography, 2nd ed, Boka Raton: Chapman & Hall/CRC.

Barreto, P.S.L.M. el at. 2002. "Efficient Algorithms for Pairing-Based Cryptosystems", Springer Berlin Heidelberg. 22nd Annual International Cryptology Conference on Advances in Cryptology, Aug. 18-22, 2002, pp. 354-368.

Groves, M.2012. "Ellipltic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI)," RFC Editor, California, RFC 6507, Feb.pp. 1-17.

Groves, M. 2012. "Sakai-Kasahara Key Encryption (SAKKE)," RFC Editor, California, RFC 6508, Feb., pp. 1-21.

Mahapatra, R. P., Yaday, R.K. 2015. "Descendant of LEACH Based Routing Protocols in Wireless Sensor Networks", Procedia Computer Science, vol. 57, Aug., pp. 195-215.

3GPP, 2009. "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS)," 3rd Generation Partnership Project (3GPP), TS. 24.301, Release 8. Mar, pp. 1-250.

Barker, E. B., Dang, Q. H. 2015. "Application-Specific Key Management Guidance", NIST SP, 800-57, Pt. 3, Rev. 1 , Jan.

Cohen, H., Frey, G., Avanzi, R. M. 2006. Handbook of Elliptic and Hyperelliptic Curve Cryptography, Boka Raton: Chapman & Hall/CRC.

Silverman, J. H. 2008. The Arithmetic of Elliptic Curves, 2nd ed, New York: Springer.

Joux, A. 2002."The weil and Tate pairings as building blocks for public key cryptosystems", Springer Berlin Heidelberg. International Symposium, ANTS-V Sydney, Australia, June. 7-12, pp. 20-32.

****