SECURE PROTOCOL FOR FOUR D2D SCENARIOS

Hoda Nematy

[1]Malek-Ashtar University of Technology, Shabanlou,
Babaee Hwy, Lavizan, Tehran, Iran.

ABSTRACT

In traditional cellular infrastructure, cellular devices communicate with each other directly even when they are close together. This strategy causes massive traffic to the cellular network therefore D2D communication has introduced to overcome this issue, bring more bandwidth and also higher rates to the cellular network. One of the major challenges for D2D Communication is to have one single secure protocol that can adapt in four D2D scenarios defined in references. These scenarios are Direct D2D and relaying D2D communication with and without cellular infrastructure. In this paper, we propose a Secure D2D protocol based on ARIADNE with TESLA. Also we use LTE-A AKA protocol for authentication and key agreement procedure between Source and Destination. Next, we adapt this scenario to be applicable in without cellular infrastructure ones. This protocol could be used in direct D2D also. Based on the results, our proposed protocol has a few computation overhead compare to recent works and have less communication overhead than SODE with preserve many security properties such as Authentication, Authorization, Confidentiality, Integrity, Secure Key Agreement, Secure Routing Transmission…. We check Authentication, Confidentiality, Reachability and Secure Key Agreement of the proposed protocol with ProVerif verification tools.

KEYWORDS

5th generation, Four D2D scenarios, LTE-A AKA protocol, secure D2D protocol, ProVerif.

1. INTRODUCTION

D2D is a new form of communication for reducing cellular traffic and increasing the efficiency of the cellular network. This form of communication has introduced for 4th cellular communication and certainly has a big role in the 5th generation. D2D communication is a technique for direct transmission between a Source and a Destination. This technique provides a few interactions between cellular phones and the central nodes (i.e. eNodeB). The aim of D2D communication is to use D2D for close distances and use cellular communication only for far enough distances [1]. D2D First used in [2] for data transmissions between nodes. Some other researches [1]–[3] use D2D for cellular communication. Based on recent researches security is an open problem in D2D communication [4].There are several security challenges for D2D communication including Authentication, Authorization, confidentiality, integrity… and a secure protocol has to address them. Our proposed protocols use ARIADNE with TESLA [5] and LTE-A key distribution system. It designed for all four communication scenarios. Four D2D scenarios including, Direct D2D with cellular infrastructure, Direct D2D without cellular infrastructure, relaying D2D with cellular infrastructure and relaying D2D without cellular infrastructure show in Figure 1. It has also been transmitted a message in the network opportunistically by adding the encrypted message to the routing packet, this is for the mobile nature of D2D devices. When users are mobile in D2D communication, they may change their location after each routing process and no

David C. Wyld et al. (Eds): CMC, NCO, SOFT, CDKP, MLT, ICAITA - 2021
pp. 21-33, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.111102

longer participate in sending and receiving messages, therefore the routing procedure needs to be done again. But in our proposed protocol, by adding the encrypted message field to the routing package, no need to redo the routing operation and users have to participate in D2D as long as sending and receiving one packet process time.

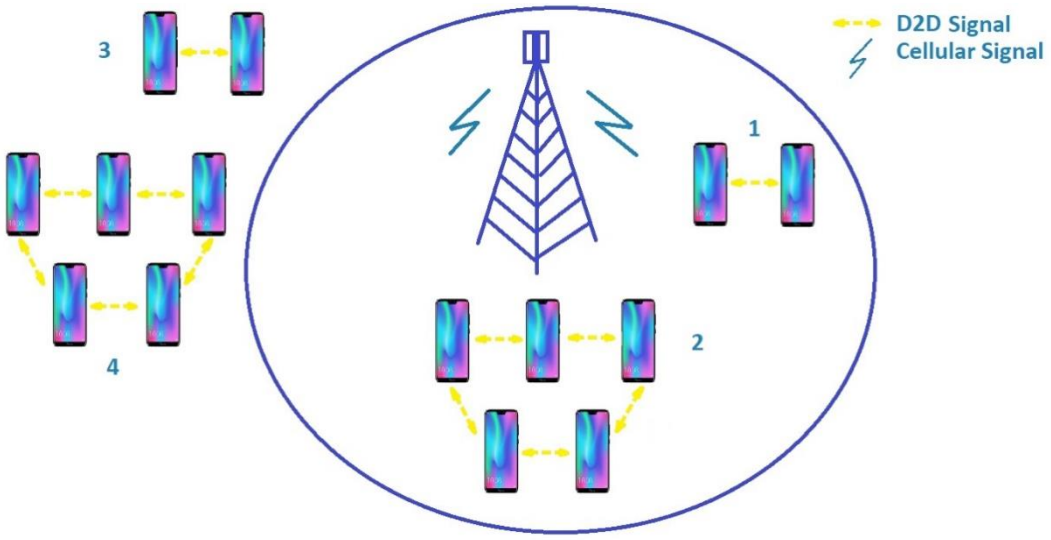

Figure 1. Four D2D Scenarios

The cellular networks may become out of reach in natural disasters, terrorist attacks, … In this scenario (out of coverage) the proposed protocol can override the network key agreement mode and use pre-shared keys. The other two ways that may be used for key agreement procedures are using the PUF circuiton D2D devices or using the Diffie-Hellman key agreement protocol. The rest of the paper is as follows. The related works come in section 2. Four D2D secure protocols with details and schematic will come in section 3 including Direct D2D Secure Protocol(DD2D), Relaying D2D Secure Protocol(RD2D), Direct D2D Secure Protocol without Cellular Infrastructure (DD2DW), and Relaying D2D Secure Protocol without Cellular Infrastructure (RD2DW). In section 4 the secure protocols will be analysed in three ways, Computation overhead, communication overhead, and security properties. In the former section, the security properties of secure protocols will discuss and the properties of Confidentiality, Reliability, one-way and two-way Authentication and Secure Key Agreement in two phases will proof with the ProVerif formal verification tool. In section 5 limitation and future works will present. Finally, the conclusion of the paper will present.

2. RELATED WORKS

The problem situation in [6] is based on a scenario in which one user covered by deactivated eNodeB wants to connect to the cellular network. In this scenario, a user in healthy eNodeB helps for communication and sharing secret keys. In this protocol two cryptic fields for each user have to be sent from each eNodeB to neighbour eNodeBs before the incident happens and every eNodeB should send these fields, to its users. In this protocol, so many communication overheads exist, because there is no information about which user may request communication and which user from the healthy network would respond to this request. Moreover, a user of healthy eNodeB may fall in the DOS attack by receiving too many requests from a malicious user. T. Ballan et al [9] use a Physically Unclonable Functions (PUF) to generate the secret key for each device. This circuit generates a unique value based on the unique character of each D2D devices, then use this unique value with the public key of another device and Elliptic Curve Cryptography to generate a

shared secret key. This sharing key is used as an input value of the Salsa20 / 20 stream cryptographic function and create a final message with the XOR operation of Salsa20/20 output and initial message. This method is prone to man-in-the-middle attacks when the attacker placed betwe en the receiver and the transmitter and sends his public key to the parties. Also, this method requires a PUF circuit that exists in both devices. L. Wang et al [10] present a distributed group key sharing scenario based on computational Diffie-Hellman (CDH) key sharing protocol in the absence of cellular infrastructure. This protocol does not provide a security solution based on the presence of an attacker within the network. Each time a user adds or eliminates from the group, a new session key should be created. P. Gope protocol [7] verifies the identity of D2D devices inside the network coverage by a middle layer called the fog layer. This middle layer connects to the core network and can authentication a device and also share a secret key with it. In another hand, the device can also verify the information received by the fog layer without disclosing its identity information to this layer. This method has been suggested to reduce the latency and to increase the mobility of end-users and could be used when a user is out of network coverage. A secure key exchange method between two D2D devices without network interference proposed in [8]. This protocol requires physical proximity of two devices before communication and for any communication physical proximity requires. In the case of reusing a key, the security of communication will be severely compromised. It is also possible to reveal the key if one of the devices is infected with malware. In [11] a secure protocol for secure communication between eNodeB and GW proposed. A summary of the security solutions of references shows in table 1.

Table 1. Security solutions in D2D communication

	Authentication	**Authorization**	**Confidentiality**	**Integrity**	**Secure routing transmission**	**Secure key agreement**	**Non-repudiation**
SOD [6]	-	-	+	-	+	+	-
LAAP [7]	+	+	-	-	-	+	+
Sec-D2D [8]	+	-	+	+	-	+	-
SDR [9]	-	-	+	-	-	+	-
CRA[10]	-	-	+	+	+	+	-

3. FOUR SECURE PROTOCOLS

We have four different protocols but the basis is the same. A Source wants to start a D2D communication to the Destination. In scenarios number 1 and 2, the Source and Destination are in each others neighboring and could receive information directly. But, in scenarios 3 and 4, the Source and Destination are not in each other neighbourhood and need the cooperation of other devices to transmit and receive information. In scenarios 1 and 3, all the devices including Source and Destination are in the cellular coverage therefore, we use the cellular advantage to distribute keys. However, for the intermediate nodes (i.e. relays), we use the TESLA broadcast authentication protocol for lessening cellular signalling traffic. In these scenarios, the Source which wants to establish a D2D communication to a specified destination sends a D2D request

including Source and Destination identity in a secure cellular channel to the MME. MME checks the validity of the message and authenticate the Source and Destination, and also checks if the destination is in the proximity of the Source or not. If all the situations above meet, MME builds a D2D session key and sends it to the Source in a secure cellular channel. Then the Source starts D2D communication towards Destination.

In ARIADNE, the packaging field includes S, D, id, and t. for Source, Destination, the ID of the message and time respectively. In this protocol, we also add the encrypted message along with the nonce. Furthermore, we use one key for evaluation of MACs instead of using two keys because the Source and destination have each other keys and one key is enough. We use the key chain TESLA protocol for intermediate users and assume that there is a system in the network where the initial values of the user's key chain are broadcast to the entire network, so every cellular device can authenticate received TESLA key. when users are in the coverage of the cellular network, this can be done by cellular network control messages. In the absence of cellular network coverage, we assume that users use the previous initial values when the cellular network was available. Our protocol in four scenarios is as follows.

3.1. Direct D2D Secure Protocol (DD2D)

In this protocol, two D2D devices are in each other vicinity and Source initiates a D2D communication by requesting the core network (MME) to establish a D2D. The pseudo code of the DD2D protocol is in pseudo code 1.Parameters used in pseudo code describes in table 2.

Pseudo code 1. Direct D2D (DD2D) Protocol

```
Start
Source:       Sends message (Request, IMSI, S, D) to MME in cellular channel
MME:          Authenticates Source and Destination
              If S & D is valid
                    If D is close enough to S
                          K= New key
                          Add [S , D] to D2D list
                          Sends K to Source
                    End if
              End if
Source:       N= New Nonce
              K'=Enc_K(N)
              C=Enc_K(m)
              H_0=MAC_K(Request, C, N, S, D, id, t)
              Source sends message (Request, C, N, S, D, id, t, H_0) to Destination in D2D channel
Destination:  If id is unique & t>=t_exp
                    Destination sends message (Request, IMSI, S, D) to MME in cellular channel
              End if
MME:          Authenticates Source and Destination
              If S & D is valid
                    If [S , D] are in D2D list
                          Sends K to Destination
                    End if
              End if
Destination:  H'_0= MAC_K(Request, C, N, S, D, id, t)
              If H'_0=H_0
                    K'= EncK(N)
                    m=Enc_K'(C)
                    M_D= MAC_K(Reply, S, D, t)
                    Destination sends message (Reply, S, D, t, M_D) to Source in D2D channel
              End if
End
```

Table 2: Parameter description

Parameter	Description
K	Secure D2D session key
$MAC_K(M)$	Message Authentication Code with the message (M) and the key (K)
$H_n()$	n^{th} Hash function in the series
$Enc_K()$	Symmetric Encryption with key K
$Dec_K()$	Symmetric Decryption with key K

3.2. Relaying D2D Secure Protocol (RD2D)

This protocol starts like DD2D by requesting a MME to establish a D2D communication from the Source. But in this scenario, the Source and the Destination are not in each others neighboring and relaying nodes should participate to transfer information. The pseudo code of the RD2D protocol is in pseudo code 2.

Pseudo code 2. Relaying D2D (RD2D) Protocol

```
Start
Source:          Sends message (Request, IMSI, S, D) to MME in cellular channel
MME:             Authenticates Source and Destination
                 If S & D is valid
                     If D is close enough to S
                         K= New key
                         Add [S , D] to D2D list
                         Send K to Source
                     End if
                 End if
Source :         N= New Nonce
                 K'=EncK(N)
                C=EncK'(m)
                H0=MAC_K(Request, C, N, S, D, id, t)
                Source sends message (Request, C, N, S, D, id, t, H0) towards Destination in D2D channel
A:               If id is unique & t>=t_exp
                     H_1=H(A, H_0)
                     M_A= MAC_KA1(Request, C, N, S, D, id, t, H_1, A)
                     A sends message (Request, C, N, S, D, id, t, H_1, A, M_A) towards Destination in D2D channel
                 End if
B:               If id is unique & t>=t_exp
                     H_2=H(B, H_1)
                     M_B= MAC_KB1(Request, C, N, S, D, id, t, H_2, A, B, M_A)
                     B sends message (Request, C, N, S, D, id, t, H_2, A, B, M_A, M_B) towards Destination in D2D channel
                 End if
C:               If id is unique & t>=t_exp
                     H_3=H(C, H_2)
                     M_C= MAC_KC1(Request, C, N, S, D, id, t, H_3, A, B, C, M_A, M_B)
                     C sends message (Request, C, N, S, D, id, t, H_2, A, B, M_A, M_B, M_C) towards Destination in D2D channel
                 End if
Destination:     If id is unique & t>=t_exp
                     Destination sends message (Request, IMSI, S, D) to MME in cellular channel
                 End if
MME:             Authenticates Source and Destination
                 If S & D is valid
                     If [S , D] are in D2D list
                         Send K to Destination
                     End if
                 End if
Destination:     H'_3=H(C, H(B, H(A, MAC_K(Request, C, N, S, D, id, t))))
                 If H'_3=H_3
                     K'= Enc_K(N)
                     m=Enc_K'(C)
                     M_D= MAC_K(Reply, S, D, t, A, B, C, M_A, M_B, M_C )
                     Destination sends message (Reply, S, D, t, A, B, C, M_A, M_B, M_C M_D) towards Source in D2D channel
                 End if
C:               C adds KCt and sends message (Reply, S, D, t, A, B, C, M_A, M_B, M_C M_D, KCt) towards Source in D2D channel
B:               B adds KBt and sends message (Reply, S, D, t, A, B, C, M_A, M_B, M_C M_D, KCt, KBt) towards Source in D2D channel
A:               A adds KAt and sends message (Reply, S, D, t, A, B, C, M_A, M_B, M_C M_D, KCt, KBt, KAt) towards Source in D2D Channel

end
```

3.3. Direct D2D Secure Protocol without Cellular Infrastructure (DD2DW)

This protocol is similar to the DD2D Protocol. However, cellular infrastructure does not exist in this protocol. To preserve confidentiality property, both Source and Destination have to use a key that sets before communication. We suppose each device already exchanged the key in a way such as key agreement procedures in [9], [10]. In the disaster situation, we suppose losing confidentiality is less important than losing vital communication. Moreover, in the situation that each if no other pre-distribution keys exist and no other procedures could be used devices can use their TESLA key. In this scenario the Destination could not validate the H_0 value before receiving the TESLA key of the source, but it can decrypt the message. So, in the case of emergency situation its better to first decrypt the package and if the TESLA key arrives and the package fails to validate then the Destination withdraws the packet. The protocol pseudo code is in the pseudo code 3.

Pseudo code 3. Direct D2D Protocol Without Cellular Infrastructure (DD2DW)

```
Start
Source:        C=Enc_K(m)
               H_0=MAC_K(Request, C, N, S, D, id, t)
               Source sends message (Request, C, N, S, D, id, t, H_0) to
               Destination in D2D channel
Destination:   If id is unique & t>=t_exp
                   H'_0= MAC_K(Request, C, N, S, D, id, t)
                   If H'_0=H_0
                       m=Enc_K(C)
                       M_D= MAC_K(Reply, S, D, t)
                       Destination sends message (Reply, S, D, t, M_D) to
                       Source in D2D channel
                   End if
               End if
End
```

3.4. Relaying D2D Secure Protocol without Cellular Infrastructure (RD2DW)

This protocol is a combination of RD2D and DD2DW, the Source and Destination are not in each other's vicinity so relaying nodes should participate in communication and also the cellular infrastructure is not available. We suppose Source and Destination already exchanged keys in a way such as explained in DD2DW. The protocol pseudo code is in pseudo code 4.

Pseudo code 4. Relaying D2D Secure Protocol without Cellular Infrastructure (RD2DW)

Start
Source: $C=Enc_K$ (m)
$H0=MAC_K$(Request, C, N, S, D, id, t)
Source sends message (Request, C, N, S, D, id, t, H0) towards Destination in D2D channel
A: If id is unique & $t>=t_{exp}$
$H_1=H(A, H_0)$
$M_A= MAC_{KAt}$(Request, C, N, S, D, id, t, H_1, A)
A sends message (Request, C, N, S, D, id, t, H_1, A, M_A) towards Destination in D2D channel
End if
B: If id is unique & $t>=t_{exp}$
$H_2=H(B, H_1)$
$M_B= MAC_{KBt}$(Request, C, N, S, D, id, t, H_2, A, B, M_A)
B sends message (Request, C, N, S, D, id, t, H_2, A, B, M_A, M_B) towards Destination in D2D channel
End if
C: If id is unique & $t>=t_{exp}$
$H_3=H(C, H_2)$
$M_C= MAC_{KCt}$(Request, C, N, S, D, id, t, H_3, A, B, C, M_A, M_B)
C sends message (Request, C, N, S, D, id, t, H_2, A, B, M_A, M_B, M_C) towards Destination in D2D channel
End if
Destination: If id is unique & $t>=t_{exp}$
$H'_3=H(C, H(B, H(A, MAC_K$(Request, C, N, S, D, id, t))))
If $H'_3=H_3$
$m=Enc_K(C)$
$M_D= MAC_K$(Reply, S, D, t, A, B, C, M_A, M_B, M_C)
Destination sends message (Reply, S, D, t, A, B, C, M_A, M_B, M_C M_D) towards Source in D2D channel
End if
End if
C: C adds KCt and sends message (Reply, S, D, t, A, B, C, M_A, M_B, M_C M_D, KCt) towards Source in D2D channel
B: B adds KBt and sends message (Reply, S, D, t, A, B, C, M_A, M_B, M_C M_D, KCt, KBt) towards Source in D2D channel
A: A adds KAt and sends message (Reply, S, D, t, A, B, C, M_A, M_B, M_C M_D, KCt, KBt, KAt) towards Source in D2D Channel

end

4. ANALYSIS OF THE PROPOSED PROTOCOLS

The amount of operations based on the role and the packet size of each node is in table 3. In this table Enc is for encryption, Dec is for decryption, H is for hash value, Ks is for key size, and n is for the number of nodes including Source and Destination. We assume symmetric encryption with the output of 256 bits and also a hash function with the size of 256 bits, 4 bits for request, ti, I, N and 8 bits for Source and Destination identities. Based on the number of nodes participating in D2D, the replay packet will have a different size. If we assume the maximum number of nodes is 20, the maximum packet size of Destination in the replay packet is 629 bytes and also the maximum packet size of intermediate nodes in request and replay packet respectively are 662 bytes and 629ks bytes.

Table 2: Operations and packet size in proposed protocols

Device	**operations**	**Packet size**
The source in direct D2D	Enc+H	544 bit
The source in relaying D2D	2Enc+H	544 bit
Destination in direct D2D	Dec+H	286 bit
Destination in relaying D2D	Enc+Dec+nH	28+(n-2)8+(n-1)256 bit
Intermediate node in the request	2H	28+(n-1)8+n256 bit
Intermediate node in the reply	-	12+8n+(n-1)256+(n-2)Ks

4.1. Computation Overhead

In the proposed protocols, we use a symmetric function for encryption and decryption of the message and one for the key evaluation parts. Also we use a cryptographic hash function for each transmission. So, there are two symmetric encryptions/decryptions, one cryptographic hash function evaluation for source and destination, and one cryptographic hash function evaluation for each relaying device. The computation cost comes in table 4 describes the proposed protocol compared to other protocols. Enc and Dec are for Encryption and Decryption, n is for the number of devices, H is a hash function, Mul is for multiplication, EO is for exponential operation, PA is for pairing, Div is for division and PO is for point multiplication.

Table 3: Computation cost of protocols

protocol	Computation cost
SDGA [12]	$3(2n-1)PA + 5nEO + (4n-1)H + 2(2n-1)Mul$
PPAKA [13]	$2(2n-1)EO + (n^2+3n-4)H + (2n^2-3n+1)Mul$
GRAAD [14]	$2nPA + 7(3n-2)H + nEnc + nDec + 3(n-1)PO + 8(n-1)EO + 2(n-1)Mul$
LRSA [15]	$6nPO + (13n-7)H + (3n-1)Mul + 2Div$
SeDS [16]	$2PA + (5n-2)EO + Dec + (2n+1)H + 4(n-1)\ PO + 2(n-1)Enc$
DD2D	$3Enc + 3H + Dec$
RD2D	$3Enc + (2n+1)H + Dec$
DD2DW	$Enc + 3H + Dec$
RD2DW	$Enc + (2n-1)H + Dec$

4.2. Communication Overhead

In RD2D and RD2DW, the protocol has 2n packet transmission for each relay device (one for Request and one for Reply). So, the communication overhead of the proposed protocol is as equation 1.

$$CommunicationOverhead = \frac{T' \times M \times (2n+2)}{T} \quad (1)$$

T' is the number of timeslots that D2D requests happen, T is the total number of timeslots, M is the number of D2D requests at each timeslot ,and n is the number of devices. We compare the communication cost of RD2D with SODE [6] because RD2D has the biggest communication overhead among the other three proposed protocols. In SODE, two cryptic fields for each device has to be sent from each eNodeBs to each eNodeB'sneighbours. Also, two cryptic fields for each neighbours have to be sent to all the devices belongs to eNodeB. Another communication parts in SODE are from D2D request and D2D reply. These two communication are for key agreement between two devices in the network. Communication overhead of RD2D and SODE based on increasing the number of time slots when the number of eNodeBs are 2 and 7 are in figures2 and 3 respectively. The communication overhead increases as the number of nodes (n) increased. When the number of eNodeBs increase to 7, the communication overhead of SODE increases for about 3 times, but in RD2D the number of eNodeBs has no effect on the communication overhead. In another comparison, we check the change of the number of T' in communication overhead when M=1 and M=5 in figures4 and 5 respectively. The communication overhead increases as T' increased and when M increases to 5 both protocols have more communication overhead. It means as the number of D2D requests increase the communication overhead

increases as well. In figure 4 and 5 RD2D has less communication overhead than SODE and the slob of SODE is much more than RD2D.

Table 4. Parameters used in communication overhead simulation

Parameter	value
n	10
T	20
T'	10
M	1 & 5

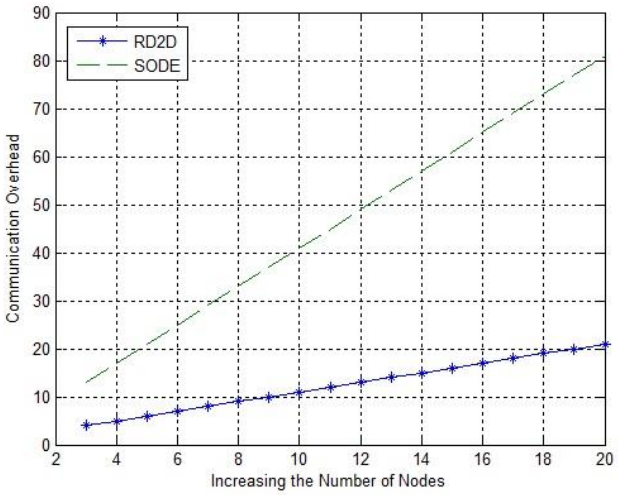

Figure 2. The Communication Overhead Vs the Number of Nodes when B=2

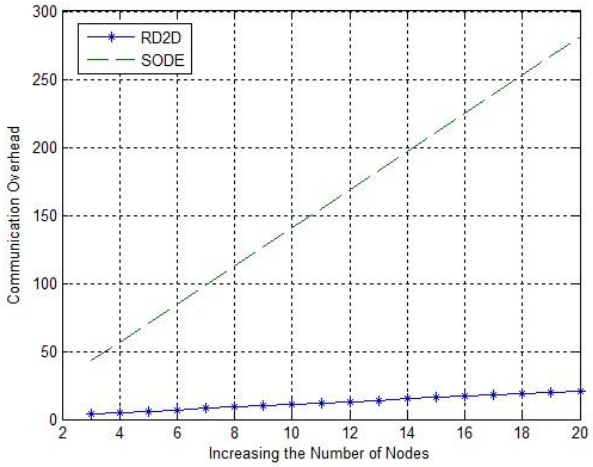

Figure 3. The Communication Overhead Vs the Number of Timeslots when B=7

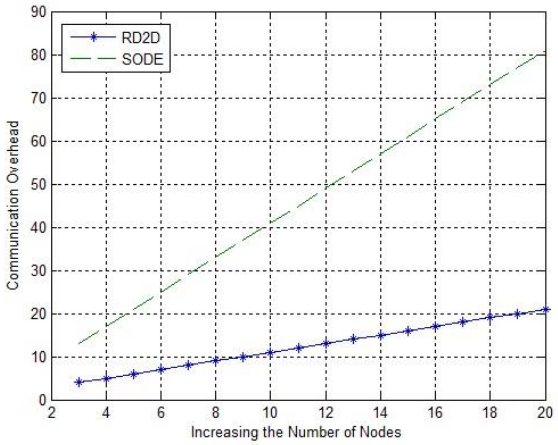

Figure 4. The Communication Overhead Vs the Number of Nodes when M=1

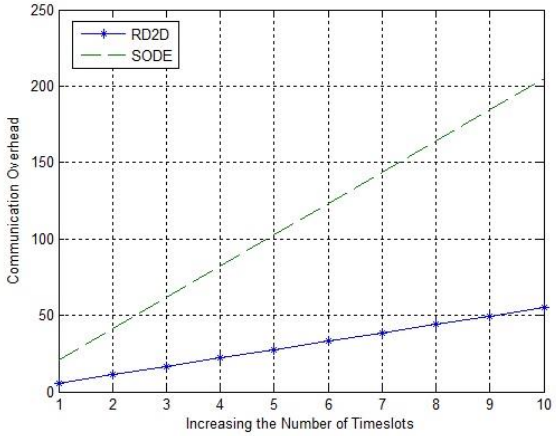

Figure 5. The Communication Overhead Vs the Number of Nodes when M=5

4.3. Security Properties of the Protocol

In this part, we show the security properties of our protocols. Our proposed protocols have Authentication, Authorization, Confidentiality, Integrity, Non-repudiation, Secure routing transmission, Secure key agreement, and reachability. We will show two more security properties Secure key agreement and reachability in the ProVerif Section and discuss the rest in this part.

1. Authentication and Authorization: This property is based on the cellular authentication and authorization process in cellular coverage scenarios (DD2D and RD2D). In two other scenarios (DD2DW and RD2DW), authentication and authorization are based on the privacy of secret keys on each side. If both sides (Source and Destination) could decrypt the packet and evaluate the message, it means both sides are authorized sides. For this assumption, we suppose that no one reveals the key and the key saved in both devices securely.
2. Confidentiality: this property is gained by the encryption and decryption of the message based on the secret key received from the MME. MME is the trusted server which would not reveal the key K to anybody but authorized Source and Destination. In DD2DW and RD2DW, the confidentiality of the message is based on the secrecy of the keys and key distribution system they used in the absence of cellular infrastructure.

3. Integrity: this property caught by the hash values. If the destination evaluates the hash chain values and they are different from what was inside the packet, it means the integrity of the packet losses and it should ignore the received packet. This property could be checked by the Source too, the field MD in reply packet does this part.
4. Non-repudiation: this property can be set by the packet id value in the request message which should be fresh. Also, t value should not be too far in the past.
5. Secure routing transmission: This property is only for RD2D and RD2DW because these two protocols have routing part. Our proposed protocols are based on ARIADNE protocol, it prevents tampering with the attackers or comprised nodes and it also resists to many Denial-of-Service attacks.

4.4. ProVerif Verification of RD2D Protocol

ProVerif is a formal tool for verifying cryptographic protocols [17]. Input language of ProVerif supports channels with the "Dolev-Yao" ability attacker. This attacker model is very strong and has full control over the channel. We use ProVerif for verifying confidentiality, reachability and secure key agreement of RD2D because it comprises three other protocols. Security properties that we use come in table 6.

Table 6. Security properties of the protocol used in ProVerif

Security Property		**ProVerif**
Confidentiality		query attacker(m).
Reachability		query event(mmeReachable()). query event(hssReachable()). query event(SourceReachable()). query event(DestinationReachable()).
Authentication	One-way authentication	event acceptsServerClientA(bitstring,key). event acceptsServerClientB(bitstring,key). event acceptsServerClientC(bitstring,key). event acceptsServerDestination(bitstring,key).
	One-to-one authentication*	event termDestination(bitstring,key).
Secure Key agreement	Running key	event SourceRunning(key). event mmeRunning(key). event DestinationRunning(key). event ClientARunning(bitstring,key). event ClientBRunning(bitstring,key). event ClientCRunning(bitstring,key).
	Key agreement	event SourceCommit(key). event mmeCommit(key). event DestinationCommit(key).

When one side of the communication checks authenticity it calls One-way authentication i.e. when Source authenticates relaying devices. However, in one-to-one authentication two sides of communication should authenticate each other i.e. Source and Destination. So we use one-to-one authentication for Source and Destination and one-way authentication for relaying devices. We check the Secure key agreement procedure in two phases, running key and key agreement. In the phase of running key, a device uses a key and in the phase of key agreement, the other device

agrees on the key used before. ProVerif verifies all the security properties of RD2D. Figure6, shows protocol verification in ProVerif.

ProVerif text output:

```
Starting query not event(SourceReachable)
goal reachable: end(SourceReachable)
RESULT not event(SourceReachable) is false.
Starting query not event(DestinationReachable)
goal reachable: end(DestinationReachable)
RESULT not event(DestinationReachable) is false.
-- Query event(SourceCommit(k_133)) ==> event(mmeRunning(k_133))
Completing...
200 rules inserted. The rule base contains 185 rules. 9 rules in the queue.
Starting query event(SourceCommit(k_133)) ==> event(mmeRunning(k_133))
goal reachable: begin(mmeRunning(kdf(n_128[imsi_127 = imsiS[!1 = @sid_35779],!1 = @sid_35780],k[!1 = @sid_35779]))) ->
end(SourceCommit(kdf(n_128[imsi_127 = imsiS[!1 = @sid_35779],!1 = @sid_35780],k[!1 = @sid_35779])))
RESULT event(SourceCommit(k_133)) ==> event(mmeRunning(k_133)) is true.
-- Query event(mmeCommit(k_134)) ==> event(SourceRunning(k_134))
Completing...
200 rules inserted. The rule base contains 185 rules. 9 rules in the queue.
Starting query event(mmeCommit(k_134)) ==> event(SourceRunning(k_134))
RESULT event(mmeCommit(k_134)) ==> event(SourceRunning(k_134)) is true.
-- Query inj-event(SourceCommit(k_135)) ==> inj-event(mmeRunning(k_135))
Completing...
```

Figure 6: ProVerif Verification of RD2D Protocol

5. LIMITATIONS AND FUTURE WORKS

There are a few researches in authentication and key agreement procedure in cellular networks and makes it hard to find resources. The problem of key distribution and key agreement procedure in disaster situations or terrorist attacks is still a challenge to be respond.

Using routing algorithms for finding intermediate nodes and combine the secure protocols and routing algorithms together would be a good improvement to this research. Moreover, a way of getting feedback from the D2D communications would be suggested in order to restrict malicious nodes and improve the communication quality. Finally, we suggest using a bonus method to increase the cooperation of intermediate nodes in the D2D communication.

6. CONCLUSIONS

We proposed four D2D secure protocols for four different scenarios (DD2D, RD2D, DD2DW, and RD2DW). This is the first time a protocol has the capability to adapt to four scenarios which are essential to D2D networks. These Protocols are based on ARIADNE with TESLA. We used LTE-A AKA protocol for Authentication and key agreement for the Source and Destination in RD2D and DD2D. Also, we used TESLA, broadcast authentication protocol, for key utilization in intermediate nodes. This protocol does not need pre-shared keys for these nodes. Based on the results, our proposed protocols have less computation overhead among recent works. RD2D has less communication overhead compare to SODE protocol and it has more communication overhead among three other proposed protocols, so the other proposed protocols have less communication overhead than SODE, too. Finally, we showed our protocol security features and proofs Confidentiality, Reachability, Authentication, Secure Key agreement with ProVerif formal verification tools. Our proposed protocols have Authentication and Authorization, Confidentiality, Integrity, Non-repudiation, Secure routing transmission, Reachability, and Secure Key agreement with low communication and computation overhead.

REFERENCES

[1] N. Kato, "On device-to-device (D2D) communication [Editor's note]," *IEEE Netw.*, vol. 30, no. 3, p. 2, 2016.

[2] Y.-D. Lin and Y.-C. Hsu, "Multihop cellular: A new architecture for wireless communications," in *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, 2000, vol. 3, pp. 1273–1282.

[3] D. Wu, L. Zhou, Y. Cai, R. Q. Hu, and Y. Qian, "The role of mobility for D2D communications in LTE-Advanced networks: energy vs. bandwidth efficiency," *IEEE Wirel. Commun.*, vol. 21, no. 2, pp. 66–71, 2014.

[4] N. Panwar, S. Sharma, and A. K. Singh, "A survey on 5G: The next generation of mobile communication," *Phys. Commun.*, vol. 18, pp. 64–84, 2016.

[5] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," *Wirel. networks*, vol. 11, no. 1–2, pp. 21–38, 2005.

[6] S. K. Tetarave and S. Tripathy, "Secure Opportunistic Data Exchange Using Smart Devices in 5G/LTE-A Networks," in *International Conference on Security & Privacy*, 2019, pp. 3–16.

[7] P. Gope, "LAAP: Lightweight Anonymous Authentication Protocol for D2D-Aided Fog Computing Paradigm," *Comput. Secur.*, 2019.

[8] M. Cao *et al.*, "Sec-D2D: A Secure and Lightweight D2D Communication System With Multiple Sensors," *IEEE Access*, vol. 7, pp. 33759–33770, 2019.

[9] T. Balan, A. Balan, and F. Sandu, "SDR Implementation of a D2D Security Cryptographic Mechanism," *IEEE Access*, vol. 7, pp. 38847–38855, 2019.

[10] L. Wang, Y. Tian, D. Zhang, and Y. Lu, "Constant-round authenticated and dynamic group key agreement protocol for D2D group communications," *Inf. Sci. (Ny).*, vol. 503, pp. 61–71, 2019.

[11] P. P. Tayade and P. Vijayakumar, "Enhancement of Security and Confidentiality for D2D Communication in LTE-Advanced Network Using Optimised Protocol," in *Wireless Communication Networks and Internet of Things*, Springer, 2019, pp. 131–139.

[12] H. Tan, Y. Song, S. Xuan, S. Pan, and I. Chung, "Secure D2D group authentication employing smartphone sensor behavior analysis," *Symmetry (Basel).*, vol. 11, no. 8, p. 969, 2019.

[13] M. Wang and Z. Yan, "Privacy-preserving authentication and key agreement protocols for D2D group communications," *IEEE Trans. Ind. Informatics*, vol. 14, no. 8, pp. 3637–3647, 2017.

[14] R.-H. Hsu, J. Lee, T. Q. S. Quek, and J.-C. Chen, "GRAAD: Group anonymous and accountable D2D communication in mobile networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 2, pp. 449–464, 2017.

[15] A. Zhang, L. Wang, X. Ye, and X. Lin, "Light-weight and robust security-aware D2D-assist data transmission protocol for mobile-health systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 3, pp. 662–675, 2016.

[16] A. Zhang, J. Chen, R. Q. Hu, and Y. Qian, "SeDS: Secure data sharing strategy for D2D communication in LTE-Advanced networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2659–2672, 2015.

[17] B. Blanchet, B. Smyth, V. Cheval, and M. Sylvestre, "ProVerif 2.00: Automatic Cryptographic Protocol Verifier, User Manual and Tutorial," *Version from*, pp. 5–16, 2018.

AUTHORS

Hoda Nematy is an Electrical Engineer, having graduated from the Malek-Ashtar University of Technology with a M.S degree in Cryptography and Safe Communication. Currently, she is working as the R&D team manager in the Pars Pooya Control Binalood Co.