ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8, August 2017

Simple & Secure Mechanism for establishing connection between D2D Communication in 5G Scenario

[1] Rajakumar Arul, [2] Gunasekaran Raja, [3] Ramkumar Jayaraman
[1] Research Scholar, [2] Associate professor, [3] Research Scholar

***Abstract*— When the wireless technologies are moving from LTE to LTE-A, the high data rate is considered in D2D communication i.e. 5G. In a network, Network server and multiple devices play a major role in information exchange. There are several challenges faced by the users and also network such as information exchange by the intruders, authentication failure, data dissemination, etc. The paper focuses on the two approaches such as information exchange from the network to device and device to device i.e. D2D along with authentication establishment. One approach dealt with authentication and encryption scheme which is already used in LTE netwo rks. Our propose focuses mainly on the device to device based on network authentication and symmetric key exchange for secure access i .e. SIE protocol. For performance analysis, AVISPA is used as the protocol checker to verify whether the proposed protocol is safe or not. The results supports our claim and proves the protocol to be safe under the assumed scenario.**

***Index Terms*— LTE-A, Authentication, Information exchange, D2D Communication.**

I. INTRODUCTION

5G evolution is the primary target in the year 2020. 5G can be possible only if all our current technologies are clubbed in such a way that there is no flaw. By seeing the technical evolution, it is well known that D2D (Device to Device) plays a key role in the forthcoming 5G network. Mainly D2D is referred as the communication between the users in the cellular networks whereas, information exchange should be more secure with high data rate i.e. LTE-A (Long Term Evolution – Advanced) [1]. LTE-A is an extended technology of LTE (Long Term Evolution) with the concern of 3GPP (Third generation partnership project). In the recent days, areas such as spectrum resource i.e. licensed and unlicensed spectrum, guaranteed QoS (Quality of Service), Data exchange, etc are the prominent issues in cellular networks.

Network is considered with multiple client and server as connection establishment and information exchange. When more and more information are diluted in wireless networks, there may be more chance of fake information exchange. So, the problem deals with secure information exchange and authentication need to be focussed [2]. Recent technology like

5G which is more and more focuses towards D2D communication where information's are exchanged in mobility condition. When D2D is concerned, it requires a Simple and Secure (S&S) communication when D2D is initiated [3]. In this paper, we propose an S&S mechanism, which dealt with two schemes such as, Device to Network

and Device to Device communication. In Device to Network communication, authentication and encryption schemes are processed which are already used in LTE network. Mainly, we focus on Device to Device Communication, where authentication process and symmetric key exchange are used for secure accesses that are highlighted as SIE protocol. Here, network, intruders and multiple devices are participated in the protocol to make it secure and safe for information exchange.

Rest of the paper is organised as follows: existing surveys are summarized in section 2. In section 3, problem definition is discussed. Proposed mechanisms along with two schemes are detailed in section 4. The performance of the mechanism are analysed in section 5 and finally, the conclusion is given in section 6.

II. RELATED WORKS

For effective communication mechanism with improved packet delivery with multiple sources and destination i.e. multicast schemes, group communication based applications are considered [4] [5]. In group key

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8, August 2017

management, challenges are classified based on centralized, distributed and decentralized environment. Several key management schemes are proposed based on user and server basis based on several multicast network structures [6]. Several schemes are surveyed and analysed based on communication and computational overhead, reliability, scalability and service management.

Regarding the key management, Abdalhossein Rezai et. al. propose a new key management scheme for secure communication [7]. In the key management, master and slave communication are initiated, and sessions are generated using elliptic curve Diffie-Hellman protocol. In the information exchange process, data is play a major role to provide security and privacy. In the health care scenarios [8], the problem of vulnerable attacks is possible while accessing some information of the patients through cloud. Propose a key management scheme to verify whether it is secure or not through various attacks i.e. location and time. Based on this key management, patients monitoring through mobile make it effective and more prevalent to the patients. Whenever the key management is more secure, authentication scheme are used to make the users who are approaching as authenticated. New authenticated key agreement scheme [9] is proposed to traverse the information more secure without any leakage with some encrypted data scheme. In this scheme, various diffie hellman key exchange security scheme are used to make session generator more effective. Jin-Hee Cho et. al. [10] proposes a trust based key management with performance maximization to mitigate the security during vulnerable condition. Performance are analysed based on trust and risk with maximized services and tolerable communication overhead.

Regarding authentication scheme among the users in the network, PGP (Pretty Good Privacy) based trust model has effective feature which requires trusted parties request [11]. Author imposes on new PGP based trust with certificateless scheme based on cryptography and to make participated nodes more trustable in the network. Analysis mainly concentrated on the improvement of communication, computation cost and storage capacity is maintained. In the above mechanism are related to previous technologies like MANETs, WiFi, WSN (Wireless Sensor Networks) [12] etc. but nowadays, network technologies are moving towards LTE and LTE-A i.e. 5G. Moving to LTE and LTE-A, user experience and resource utilization is the prominent challenges among the users to each other. Several enhanced network architecture are proposed [13] to extend LTE-A with strengthened services. Concept dealt with LTE-A enhancement integrated with D2D communication along with cloud services. As LTE-A architecture is focused with D2D communication [14].

III. PROBLEM DEFINITION

In LTE-A network, D2D communication has more user participants where users are moving with high mobility for information exchange. During these processes, there is a prominent challenge for the network to secure the information and authenticate the users whether they are trusted users or vulnerable users. For D2D communication, proposed protocol on authentication which are secure based on three parameters such as, prime 'p', base 'b' and symmetric key 'KX' along with pseudo random generator to make it unpredictable for the intruder to access the network information. After connection gets established, encryption scheme gets into role to make the information encrypted. Analysis of the protocol is validated whether it is safe ot not when the intruders are present in the network.

IV. SIMPLE AND SECURE MECHANISM

A. Network to device approach

As shown in Figure 1, when communication between the Network to device is initiated, Authentication and encryption scheme use same procedure as in LTE (Long Term Evolution) networks [15] [16].

B. Device to Device approach

Authentication management and Information exchange between Device to Device (D2D).

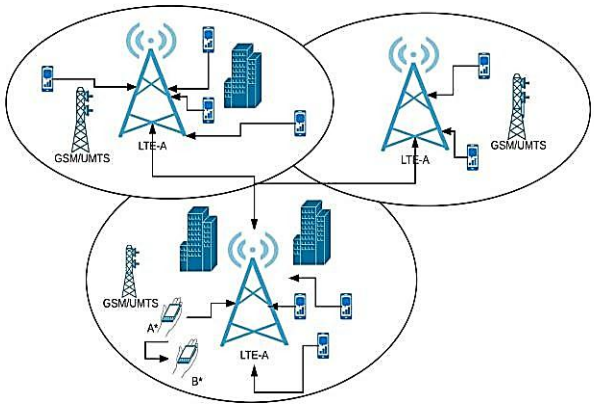

Fig. 1 D2D archieture in LTE/LTE-A Networks

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8, August 2017

1. *Encryption and Authentication*

Our contribution focus on phase 2, D2D communication when any D2D device initiates authentication and faster service renewal. To support the authentication, the network broadcasts three authentication parameters such as prime 'P', base 'g' and a symmetric key KX {g, P, KX} to all nearby D2D devices, by which they can compute random number 'Ra' and 'Rb' using pseudo random number generator to request for Aut_Req between device 'D1' and 'D2'as shown in Fig. 2. The Aut_Req request is sent from both the devices D1_id and D2_id with {gRand, Ra} &{gRand, Rb}. On receiving the request, both devices generate corresponding random numbers and will perform a validity check by which if Ra = Rb then the authentication is successful and the D2D devices are given mutual access.

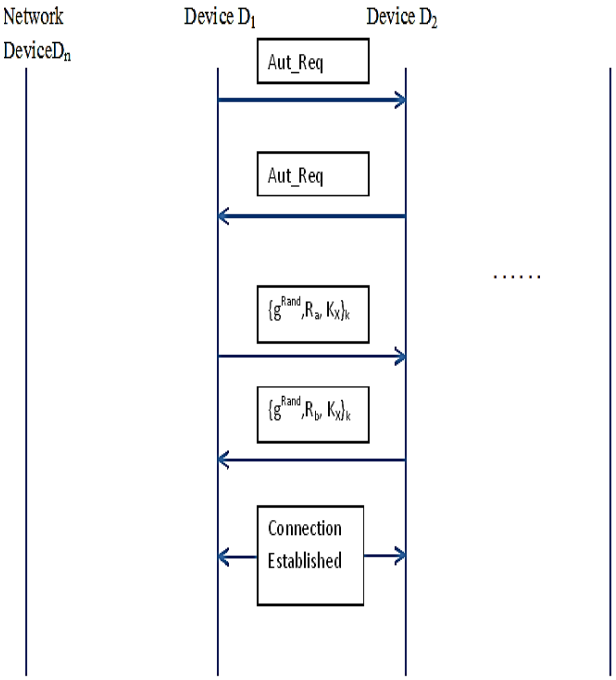

Fig. 2 Messege between different devices

Message exchanges involved are,

1. Aut_Req→ { D_1_id,Nw_id, g^{Rand}, R_a } as key 'K'
2. Aut_Req→ { D_2_id,Nw_id, g^{Rand}, R_b } as key 'K'
3. Authentication → { g^{Rand}, R_a, K_X}
4. Authenticated →{ g^{Rand}, R_b, K_X}
5. Connection Establishment → Check {$g^{Ra, Rb}$} both the sides. If it matches, authentication is successful.
6. Encryption { $g^{Ra, Rb}$}$_k$ for Key 'K'

V. PERFORMANCE ANALYSIS

The proposed mechanism is analysed using the security protocol verification tool AVISPA. The Analysis clearly suggests that our proposed Key Management & Authentication Mechanism is safe against Man-in-the-Middle attack, DoS and Replay Attack. Rogues Base station Attack seems to be possible. Here Network elements are not sent over the radio and also at no point the elements received from the network are sent between the devices so a rouge device cannot get access to the network.

A. *Possible Attacks [17]:*

1. If a node of the network is compromised then through that node the elements of the nodes can be obtained and all the data of the network can be hacked.
2. At any point the Paramets which are obtained from the Network side must not revealed by anyone in the Network.

B. *Complexity Analysis [18]:*

Through this mechanism, we can drastically minimize a dedicated Key generation for both the sides. Also here we are doing both Authentication and Key Exchange by a single method so no need of 2 separate procedures.
When, In an Environment like mesh for creating the initial network topology all the devices has to be authenticated. Only after Authentication, the network topology is formed. After forming the topology, the routing table is updated. In general for the Mesh network types, the complexity analysis as follows

C. *Key Generation [19]:*

If the Key Size is 'sk' and the key generation function involves only basic arithmetic operations then it takes the complexity O(n).
Also for Key exchange [20], we have to send the computed key over the network by encrypting it with a key.

O(n) – for creating the Encryption key
O(n) – for Key Exchange O(n)- Message Exchanges O(1)- for Encryption process
So,
Complexity = O(n) * O(n) * O(n) * O(1)
= O(n3) + O(n)

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8, August 2017

O(n) – for Authentication Process

So, by the traditional mechanism it takes at least O(n2) for the overall procedure of Authentication.

In our proposed Authentication Cum Key exchange mechanism, complexity Analysis is as follows.

O(1) – for Encryption key Exchange
O(log n) – for key generation
O(log n) – for Authentication process

So when you consider the computational cost of our proposed method,

Complexity = O(log n) * O(log n) * O(1)
= O(log n)

Our proposed algorithm is tested in AVISPA tool and found it is safe from all major attacks. Significantly it reduces the number of messages that are required dedicatedly to exchange Key and Authentication.

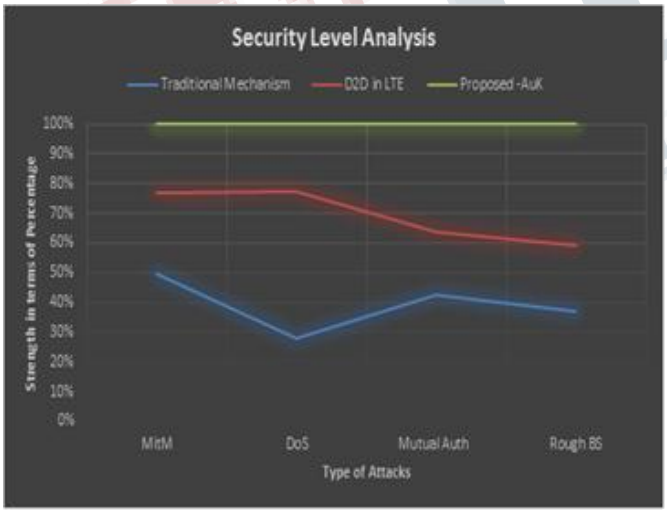

Fig. 3. Security Level Analysis of Authentication and Key agreement protocols

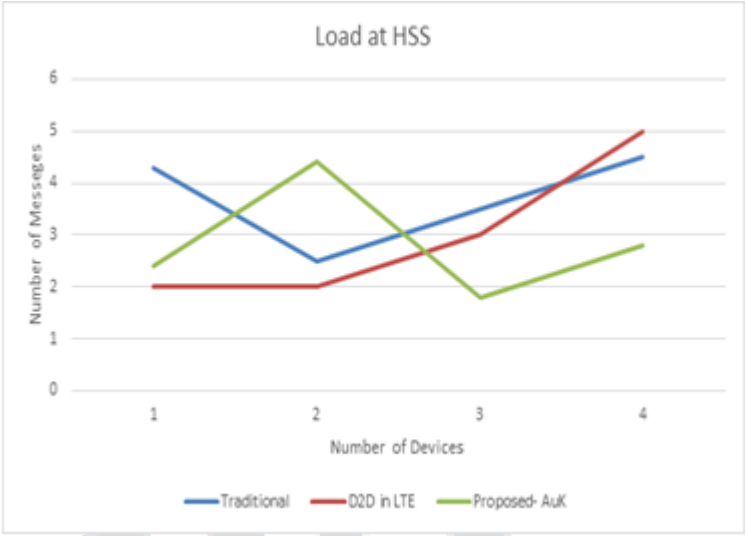

Fig. 4 Load at HSS

Fig. 3 shows the security level of proposed algorithm and found to efficient when compared to the traditional key management protocols. Fig.4 depicts the load imposed on HSS as a result of deploying AuK over HSS. We infer from the Fig.4 that only a considerable delay is imposed on HSS. So it is acceptable in terms of operational expenditure

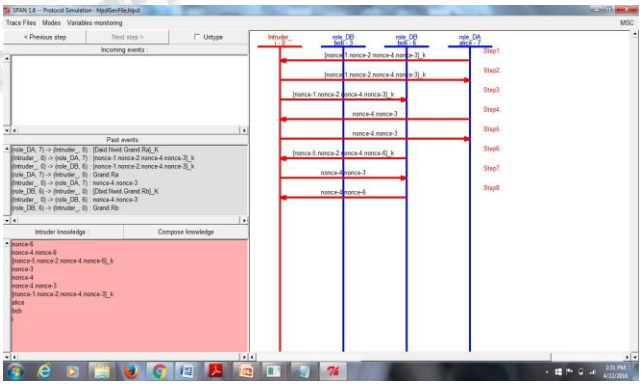

Fig. 5 AVISPA intruder simulation model

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8, August 2017

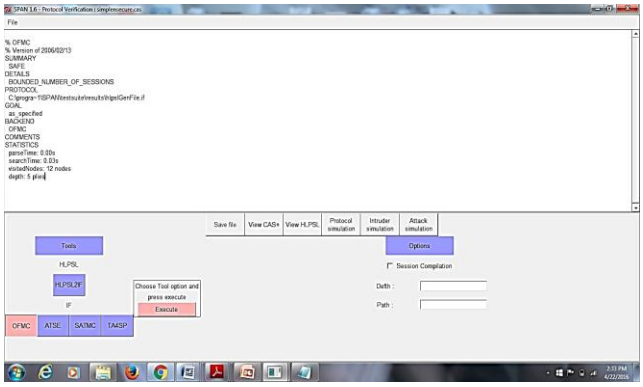

Fig. 6 AVISPA protocol description after execution

Fig. 5& Fig. 6 proves our claim and shows our proposed mechanism is rigid in all intruder simulation and safe against various attacks.

VI. CONCLUSION

Thus our proposed mechanism solves the problem of mutual authentication and provides secure way to connect

two devices. Also the computational load imposed on the system is also less when compared to the complex security algorithms. Our mechanism is well and good in terms of both computation and cost. The future scope of this protocol is aimed to be deployed under crowd-sourced environment and in places where a sudden bursty traffic arises.

REFERENCES

1. Ian F. Akyildiz, Shuai Nie, Shih-Chun Lin, Manoj Chandrasekaran, "5G roadmap: 10 key enabling technologies", Computer Networks, Elsevier Publications, Vol. 106, pp. 17 – 48, 2016.

2. Emad Abd-Elrahman, Hatem Ibn-khedher and Hossam Afifi, "D2D Group Communications Security", International Conference on New Technologies of Distributed Systems (NTDS), 2015 International Conference on Protocol Engineering (ICPE), 2015.

3. Mingjun Wang & Zheng Yan," Security in D2D Communications: A Review", IEEE Trustcom/BigDataSE/ISPA, 2015.

4. Rongqing Zhang, Member, IEEE, Xiang Cheng, Senior Member, IEEE, and Liuqing Yang, Fellow, IEEE, "Joint Power and Access Control for Physical Layer Security in D2D Communications Underlaying Cellular Networks" IEEE Conference on Communication, ICC 2016.

5. Lei Xu, Chunxiao Jiang, Yanyao Shen, Tony Q. S. Quek, Zhu Han and Yong Ren, "Energy Efficient D2D Communications: a Perspective of Mechanism Design", IEEE Transactions on Wireless Communications, Vol. 51, Issue. 11, pp. 7272 – 7285, 2016.

6. Hwayoung Um and E.J. Delp, "A Secure Group Key Management Scheme for Wireless Cellular Networks," Third International Conference on Information Technology: New Generations, ITNG 2006.

7. Abdalhossein Rezai, Parviz Keshavarzi and Zahra Moravej, "Key management issue in SCADA networks: A review," an International Journal Engineering Science and Technology, Vol. 21, Isuue. 1, pp. 354 – 363, 2017.

8. Pardeep Kumar and Hoon-Jae Lee, "Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey," Journal of Sensors, Vol. 12, Issue. 1, pp. 51 – 91, 2012.

9. Vanga Odelu, Ashok Kumar Das, Mohammad Wazid and Mauro Conti, "Provably Secure Authenticated Key Agreement Scheme for Smart Grid," IEEE Transactions on Smart Grid, Vol. PP, Issue. 99, 2016.

10. Jin-Hee Cho, Ananthram Swami and Ing-Ray Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks,"

11. Alfarez Abdul-Rahman, "The PGP Trust Model", the Journal of Electronic Commerce, 1997.

12. Theodore Zahariadis, Helen C. Leligou, Panagiotis Trakadas and Stamatis Voliotis, "Trust management in wireless sensor networks," Transactions on Emerging Telecommunications Technologies, Wiley, Vol. 21, Issue. 4, pp. 386-395, 2010.

13. Klaus Doppler, Mika Rinne, Carl Wijting, Cassio B. Ribeiro and Klaus Hugl, "Device-to-device communication as an underlay to LTE-advanced networks," IEEE Communications Magazine, Vol. 47, Issue. 12, 2009, Doi: 10.1109/MCOM.2009.5350367.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8, August 2017

14. Takehiro Nakamura, Satoshi Nagata, Anass Benjebbour, Yoshihisa Kishiyama, Tang Hai, Shen Xiaodong and Yang Ning Li Nan, "Trends in small cell enhancements in LTE advanced," IEEE Communications Magazine, Vol. 51, Issue. 2, pp. 98-105, 2013.

15. Anastasios N. Bikos and Nicolas Sklavos, "LTE/SAE Security Issues on 4G Wireless Networks," IEEE Security & Privacy, Vol. 11, Issue. 2, pp. 55-62, 2013.

16. JinCao, HuiLi, MaodeMa, YueyuZhang and ChengzheLai, "A simple and robust handover authentication between HeNB and eNB in LTE networks," Computer Networks, Elsevier Publications, Vol. 56, Issue. 8, pp. 2119-2131, 2012.

17. Younghun Chae, Lisa Cingiser DiPippo and Yan Lindsay Sun, "Trust Management for Defending On-Off Attacks," IEEE Transactions on Parallel and Distributed Systems, Vol. 26, Issue. 4, pp. 1178-1191, 2015.

18. Hong Fan, Zhu Xian and Wang Shaobin, "Delegation depth control in trust-management system," 19th International Conference on Advanced Information Networking and Applications, AINA 2005.

19. Saju PJohn and PhilipSamuel, "Self-organized key management with trusted certificate exchange in MANET," Ain Shams Engineering Journal, Vol. 6, Issue. 1, pp. 161-170, 2015.

20. Eun-Jun Yoon and Kee-Young Yoo, "Cryptanalysis of a simple three-party password-based key exchange protocol," International Journal of Communication Systems, Wiley, Vol. 24, Issue. 4, pp. 532-542, 2011

AUTHOR BIOGRAPHY

RajaKumar Arul pursued his Bachelor of Engineering in Computer Science and Engineering from Anna University, Coimbatore. He received his Master's in Computer Science and Engineering at Anna University - MIT Campus. Currently, he is pursuing Doctorate of Philosophy under the Faculty of Information and Communication in NGN Labs, Department of Computer Technology, Anna University - MIT Campus. He is a recipient of Anna Centenary Research Fellowship. His research interests include Security in Broadband Wireless Networks, WiMAX, LTE, Robust resource allocation schemes in Mobile Communication Networks.

Gunasekaran Raja is an Associate Professor in Department of Computer Technology at Anna University, Chennai and also the Principal Investigator of NGNLabs. He received his B.E degree in Computer Science and Engineering from University of Madras in 2001, a M.E in Computer Science and Engineering from Bharathiyar University in 2003, and the Ph.D in Faculty of Information and Communication Engineering from Anna University, Chennai in 2010. He was a Post-Doctoral Fellow from University of California, Davis, USA, 2014-2015. He was a recipient of Young Engineer Award from Institution of Engineers India (IEI) in 2009 and FastTrack grant for Young Scientist from Department of Science and Technology (DST) in 2011. Current research interest includes 5G Networks, LTE-Advanced, Wireless Security, Mobile Database and Data Offloading. He is a member of IEEE, Senior member of ACM, CSI and ISTE.

Ramkumar Jayaraman received B.Tech. degree in Information Technology from Anna University, Chennai in 2009 and M.E.in Computer Science and Engineering from Anna University, Coimbatore in 2011. He is currently doing Doctorate of Philosophy program under the Faculty of Information and Communication in NGN Labs, Department of Computer Technology, Anna University - MIT Campus. He is a recipient of Anna Centenary Research Fellowship. His key research areas of interests are Broadband Wireless Networks and Scheduling in WiMAX.