International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 3, Issue 4, April 2016

Improving Security and QOS in Device-To-Device Communication Using Elliptic Curve DIFFIE Hellman Algorithm

[1] DR. D. Karunkuzhali [2] G. Vidhya Sri [3] D. Thilagavathi [4] S. Suvetha [5] M. Aswini
[1] Associate Professor [2][3][4][5] Student
[1][2][3][4][5] Department of IT
Panimalar Engineering College
[1] karunkuzhali@gmail.com [2] vidhyasri95@gmail.com [3] thilaks2013@gmail.com
[4] suve2008suvetha@gmail.com [5] aish31aswini@gmail.com

Abstract: **with the fast development of Device-to-Device (D2D) communications in 4G LTE-Advanced networks and increase in use of smart phone and tablet users, D2D has become an appealing solution for enhancing the security performance of traditional cellular networks. In this paper we enhance the security requirements by implementing Elliptic Curve Diffie Hellman (ECDH) algorithm in D2D. This anonymous key agreement protocol allows two parties to establish a shared secret over an insecure channel. We integrate our proposed protocol into the existing Vehicular Connection Steering (VECOS) Protocol and execute it using simulation.**

***Index terms*- D2D communications; LTE- Advanced networks; security; ECDH algorithm; key agreement protocol; VECOS protocol**

I. INTRODUCTION

Device-to-Device (D2D) communications refers to direct short-range communications between terminals of a mobile network and this doesn't include the intermediate transmission to a base station (BS). Varying from conventional approaches like Bluetooth and WiFi-Direct. D2D communications utilize licensed spectrum with quality of service (QoS) assures that no manual network detection and network selection is required. Comparing with existing radio communications secondary transmissions are allowed simultaneously in cellular (primary) transmissions, D2D communications are constituted by cellular (primary) users that are deriving the benefits of being synchronized and controlled by the Base Station. D2D communications have been instigated to offload the traffic burden from cellular infrastructure to personal devices [1]. The D2D technology enables mobile mechanism users directly institute wireless links between every single supplementary, lacking bypassing across the public cellular infrastructure or access points.

Device-to-Device (D2D) contact has been target to be a enthusing data offloading resolution[12] and spectrum efficiency enhancement method due to its underlying characteristics, e.g., enhancing resource utilization, enhancing user's throughput, spreading battery lifetime, etc.[2]-[6] Upholding the decent quality of service (QoS) and quality of experience (QoE) Of LTE services for a user on board a vehicle in movement is a challenging setback and a way for that is to anticipate QoS and QoE degradation and to exploit the disparate wireless admission technologies, like Wi-Fi, that could be obtainable at an LTE- connected vehicle Or, in finish, at an LTE the user supplies (User Equipment) board the vehicle. To select the best QOS admission point, Vehicular Connection Steering (VECOS) protocol provides the enthusing resolutions by two disparate models, counseled to select the web selection progress. The early one is established on the (MADM) Multi Attribute Decision Making method and the subsequent ideal is established on the (MDP) Markov Decision Process. Elliptic Curve Diffie Hellman (ECDH) is an anonymous key agreementprotocol that allows two parties to exchange a shared secret over an insecure channel where each party having an elliptic curve public-private key pair. The below figure shows the different types of elliptic curves,

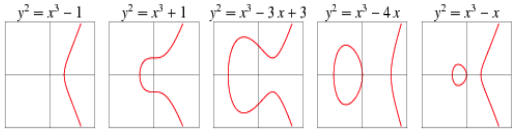

Figure 1.1-Different types of elliptic curves

II. RELATED WORK

Despite all the benefits of D2D contact, security is one of the main concerns that demand to be well addressed before D2D method gets extensively consented and implemented. It is well recognized that due to the nature of wireless channels, wireless contact such as Wi-Fi and Bluetooth is vulnerable to a collection of aggressions that trials the three frank principles of security confidentiality, integrity and availability. A little public attack vectors contain surreptitious eavesdropping, memo modification and node impersonation. For example, by stealthy listening to the communication between two mechanisms, an attacker can gain critical or privacy information, such as transactions secrets or individuality connected information. Thus, the D2D contact amid mechanisms demands to be properly secured.

To safeguard the D2D contact, cryptography solutions are demanded to encrypt the memos as they are transmitted via wireless channels. Countless encryption algorithms have been well industrialized that can furnish disparate security levels for the encrypted memos, but all of them require two mechanisms concur on a public hidden (either a public secret key or every single other's area keys). Due to the colossal number of mobile mechanisms, the diversity of mechanism manufacturers and lack of standards, preloading safeguard keys into mobile devices is neither effectual nor practical. On the supplementary hand, a trusted third party or groundwork is not probable to be obtainable in the D2D mobile environment. Thus, how to institute a shared secret amid mechanisms is one of the main trials for secure D2D communications. [13] And [14] debate the physical layer resolutions for secure D2D communications, but their methods are tough to be implemented with the devices available in the market.

To grasp handoff, Liu et al. [7] counseled the Profit purpose, whereas every single handoff is associated alongside a profit that is selected by a target function with two parameters, namely, bandwidth gain and handoff cost. Parameters utilized in the calculation of the gain include 1) admission webs alongside their maximum bandwidth provided to a solitary user as well as capacity utilization, 2) application's maximum necessity on bandwidth, and 3) access networks' bandwidths utilized by a mobile node for handoff. Then, the authors described a handoff price as data volume capitulated due to handoff delay; it agrees with the volume of data that could have been sent across the handoff delay. Thus, the profit is a difference amid gain and cost. At every single handoff epoch, mobile node assesses profit from every single web and chooses the profit that yields maximum profit. This scheme takes merely bandwidth-related parameters into account. However, solely pondering bandwidth cannot promise good Quality of Experience (QoE) for multimedia applications. Employing multi attribute decision making (MADM) to enable the implementation of a vertical handover between 3GPP and Wi-Fi webs and assist UE mechanisms in selecting theoptimal wireless admission out of countless obtainable access technologies, present discussion inside 3GPP alongside stare to whether WLAN can be believed as a "trusted non-3GPP" or "untrusted non-3GPP" access. For an effectual interworking between WLAN and LTE, countless operators and vendors are in favor of qualifying WLAN as a trusted non-3GPP. There are also evolving standards hobbies on enabling seamless WLAN based offload versus non seamless WLAN-based offload [8] and on location-based selection of gateways for seamless WLAN-based offload. As the admission web invention and selection purpose (ANDSF) was primarily projected for the selection between 3GPP and non-3GPP accesses such as WLAN [9], more standards work considers the expansion of ANDSF functionalities to the selection of packet data web (PDN) connection from inside the 3GPP area and enabling UE devices to drive IP flows amid the obtainable. In [10], Nadembega *et al*. have counseled a scheme for the forecast of the whole or the partial advancing trail of a vehicle, upheld by the forecast of the final destination or the intermediate points alongside the trail established on past data, contextual knowledge and spatial conceptual maps[11].

III. ELLIPTIC CURVE DIFFIE HELLMAN ALGORITHM

Here we discuss about the implementation of the paper.

A.EDCH Algorithm

Elliptic Curve Diffie Hellman (ECDH) algorithm is used to establish a shared secret over an insecure channel. This system is merely a method for exchanging key and here no messages are involved. The ECDH algorithm, in this paper, is used for authenticating the mobile users and the access points.

The following algorithm illustrates the Elliptic Curve Diffie Hellman Key Exchange. Suppose two communications Alice and Bob, wants to agree upon a key. They first fix a finite field F_q, an elliptic curve E defined over it and base point $B \in E$. An elliptic curve E over the finite field F_P is given through an equation of the form,

$y^2=x^3+ax+b$

Where, $4a^3+27b^2 \neq 0$

To generate a key, first Alice chooses a random $a \in F_q$ which he keeps secret. Next, he calculates $aB \in E$ that is public and sends it to Bob. Bob does the same steps, i.e. she chooses a random integer b (secret) and calculates bB, that is sent to Alice. Their secret common key is then P = $abB \in E$. The step by step process is shown below,

- Alice and Bob first choose a finite field F_p and an elliptic curve E defined over it (E(Fp)).

- They publicly choose a random base point B∈E.
- Alice chooses a secret random integer e. She then computes eB∈E and sends it to Bob.

- Bob chooses a secret random integer d. He then computes dB∈E and sends it to Alice. eB and dB are public but e and d are secret.
- Alice computes the secret key edB = e(dB).
- Bob computes the secret key edB = d(eB).
- There is no fast way to compute edB if only knows B, eB, and dB. After these steps Alice and Bob have the same point, they share the message in the following manner,

Alice and Bob Compute edB = S = (s1, s2). (Using Diffie–Hellman Scheme)
Alice sends a message M∈E to Bob as follows:
Compute (s1 * s2)modN = K.
Compute K*M = C, and send C to Bob.

Bob receives C and decrypts it as follows:
Compute (s1 * s2)modN = K.
Compute (K^{-1})modN. (where N = #E)
K^{-1}*C = K^{-1}*K*M = M

B.VECOS Protocol
Vehicular Connection Steering (VECOS) Protocol is used here to monitor the mobility of user equipment in the network. The following algorithm illustrates the VECOS Protocol,

Step-1: Base station initializes the Mapping message. Broadcast out the packet.

Step-2: If Mapping message is received, check if it is the relay node, If yes (initially no subscriber station activated) Checks the mapping message for own communication,

***Step-2a*:** if there is no detail for own communication and the data is available then generate the request message to access the bandwidth.

Step-2b: If bandwidth is allocated for communication and if the data is available then transfer the data otherwise ignore the message.
Step-3: If request message is received in Base Station, Check the number of nodes connected directly (in real time, it will be like uplink/downlink sub-frame checking)

Step-3a: Check the maximum connectivity packet count(Cmax), if it has reached the max. limit then break otherwise allocate the new data access rate to generate the response message.

***Step-3b*:** If the period is for sharing the mapping message then update the detail to mapping message and ignore the response message otherwise send the response message.

Step-4: If subscriber station is activated, advertise its activated information and listen for mapping messages from relay nodes,

Step-4a: If mapping message is received, check the connection information, if it is available for own use then update the relay information as pre defined relay otherwise generate the connection request.

Step-4b: If response message is received then set the pre defined the relay for further communication.

Step-4c: If the data is ready to transfer and the pre defined relay is available then make the connection.

Step-4d: If the pre defined relay is not in the range, listen the mapping/request/response messages of other relays.

Step-4e: If the relay node is found with enough bandwidth then send the data to relay otherwise listen to the messages from base station, if enough bandwidth is available then send data directly to base station.

Step-5: If mobile relay is activated then the node will act as normal relay.

IV. EXPERIMENTAL RESULTS

1. Network Selection

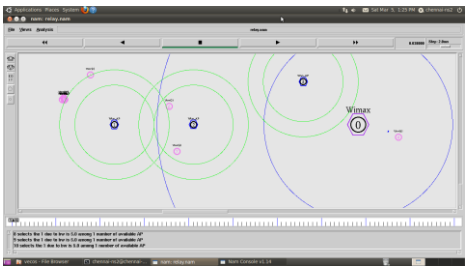

Figure 4.1-Initial topology

In initial topology, we have one 4G LTE Advanced networks(Wimax), three WLANs and several mobile users. Here the mobile users are going to interact alongside secured access point employing Elliptical Curve Diffie Hellman algorithm and selecting the best QOS access point by VECOS protocol.

2. Fading Detection

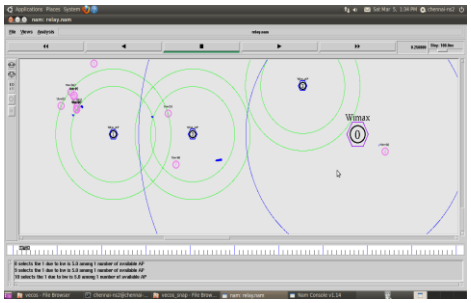

Figure 4.1-Handoff takes place

In existing system, some packets may be lost during handoff due to lack of fading detection which reduces QoS, in the fig 4.2, the user0 moves from WLAN1 to WLAN2.

3. Secured Node Selection

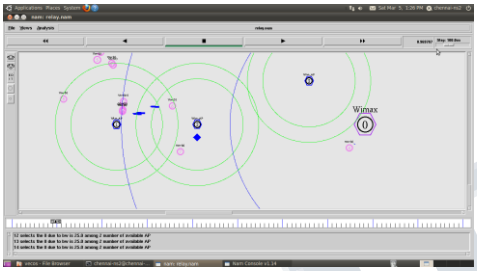

Figure 4.2-packet dropping at WLAN2 based on ECDH algorithm

In fig 4.3 based on public key comparison WLAN2 is identified as hacker node, packet dropping is recognized.

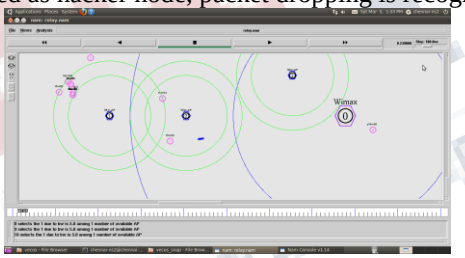

Figure** Error! No text of specified style in document.**3-Prevention of WLAN-2 with ECDH Algorithm UE-7 sends data to LTE

After identifying that the WLAN2 is hacker node, user7 directly communicates with LTE instead of WLAN2 as in fig4.4

4. Effective Handoff

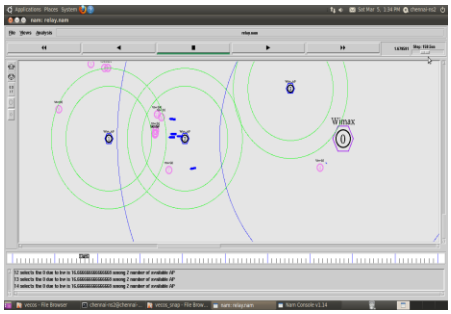

Figure 4.4-Checks VECOS Condition and Selects the best AP without considering WLAN2

Above fig4.5 depicts the selection of best AP (access point) based on the following conditions:

- Mobility path
- Bandwidth
- Link expiry time
- Number of users

Then the effective handoff takes place. These conditions are also verified during link expiry.

V. PERFORMANCE ANALYSIS

In this section, the analysis of the existing and proposed work is done as follows,

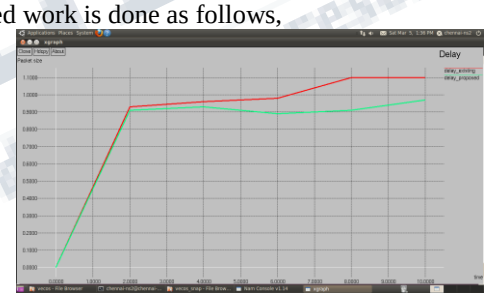

Figure 5.1-relay rate Vs time

In fig 5.1 the delay rate of the proposed system is less due to the involvement of more number of user equipments (UE).

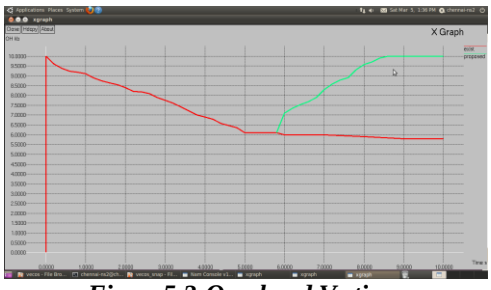

Figure5.2-Overhead Vs time

Overhead is any combination of indirect computation time, memory, bandwidth or other resources that are required to attain a goal. The overhead in proposed system is more due to the higher speed and computation of the Elliptic Curve Diffie Hellman algorithm.

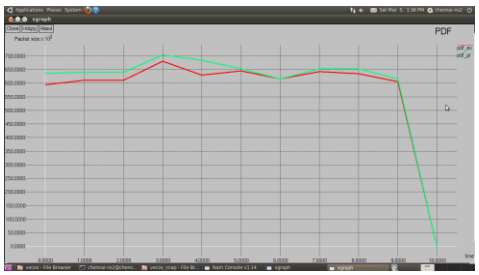

Figure 5.3-Packet Delivery Factor Vs time

Since the number of user equipment involved is more the Packet Delivery Factor is more compared to the existing system.

VI. CONCLUSION

Thus, Elliptic Curve Diffie Hellman (ECDH) algorithm integrated with Vehicular Connection Steering (VECOS) protocol for D2D communication in LTE-A network satisfies security goals in terms of integrity, entity authentication and data confidentiality and thereby increasing the Quality of Service (QoS) through monitoring the network. The experimental results prove the effectiveness and flexibility of the proposed protocol.

REFERENCES

[1] G. Fodor, E. Dahlman, G. Mildh, S. Parkvall, N. Reider, G. Miklos, and Z. Turanyi, "Design aspects of network assisted device-to-device communications," IEEE Communications Magazine, vol. 50, no. 3, pp. 170-177, 2012.

[2] D. Wu, J. Wang, R. Q. Hu, Y. Cai, and L. Zhou, "The role of mobility for D2D communications in LTE-Advanced networks: Energy VS. bandwidth efficiency," *IEEE Wireless Communications*, vol. 21, no. 4, pp. 66-71, 2014.

[3] M. Yang, S. Y. Lim, H. J. Park, and N. H. Park, "Solving the data overload: Device-to-device bearer control architecture for cellular data offloading," *IEEE Vehicular Technology Magazine*, vol. 8, no. 1, pp. 31- 39, 2013.

[4] L. Zhou, Y. Wen, H. Wang, and M. Guizani, "Resource allocation with incomplete information for QoE-driven multimedia communications," *IEEE Transactions on Wireless Communications*, vol. 12, no. 8, pp. 3733- 3745, 2013.

[5] L. Zhou, R. Hu, Y. Qian, and H.-H. Chen, "Energy-Spectrum efficiency tradeoff for video streaming over mobile Ad Hoc networks," *IEEEJournal on Selected Areas in Communications*, vol. 31, no. 5, pp. 981- 991, 2013.

[6] S. Ryu, S. Park, N. Park, and S. Chung, "Development of device-to-device communication based new mobile proximity multimedia service business models," *IEEE International Conference on Multimedia andExpo Workshops*, pp. 1-6, 2013.

[7] X. Liu, V. Li, and P. Zhang, "Joint radio resource management through vertical handoffs in 4G networks," in *Proc. IEEE GLOBECOM*, Nov./Dec. 2006, pp. 1–5.

[8] 3rd Generation Partnership Project (3GPP), "Study on S2a mobility based on GTP and WLAN access to EPC," Sophia-Antipolis, France, 3GPP Specifications TR 23.852, 2011.

[9] 3rd Generation Partnership Project (3GPP), "Architecture enhancements for non-3GPP accesses," Sophia-Antipolis, France, 3GPP Specifications TS 23.402, 2011.

[10] A. Nadembega, A. Hafid, and T. Taleb, "A path prediction model to support mobile multimedia streaming," in *Proc. IEEE ICC*, Ottawa, ON, Canada, Jun. 2012, pp. 2001–2005.

[11] A. Nadembega, T. Taleb, and A. Hafid, "A destination prediction model based on historical data, contextual knowledge and spatial conceptual maps," in *Proc. IEEEICC*,Ottawa, ON, Canada, Jun. 2012, pp. 1416–1420.

[12] G. Fodor, E. Dahlman, G. Mildh, S. Parkvall, N. Reider, G. Miklos, and Z. Turanyi, "Design aspects of network assisted device-to-device communications," IEEE Communications Magazine, vol. 50, no. 3, pp.170-177,2012.

[13] J. Wang, Ch. Li, and J. Wu, "Physical layer security of D2D communications underlaying cellular networks," Applied Mechanics and Materials, vol. 441, pp. 951-954, 2014.

[14] D. Zhu, A.L. Swindlehurst, S.A. Fakoorian, W. Xu, and Ch. Zhao, "Device-to-device communications: the physical layer security advantage." in IEEE ICASSP, 2014.