Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 7 – No. 9, November 2017 – www.caeaccess.org

Double Layer Cryptographic Protocol for Mobile Ad-hoc Networks (MANETs) by Commitment Scheme

Varun Shukla
Dept.of EC
PSIT, Kanpur
Uttar Pradesh, India

Atul Chaturvedi
Dept.of Mathematics
PSIT, Kanpur
Uttar Pradesh, India

Neelam Srivastava
Dept.of EC
REC, Kannauj
Uttar Pradesh, India

ABSTRACT
In the modern world, with the ever-increasing demand of internet, the role of Cryptography becomes vital. We use e-commerce (business to consumer or consumer to business), financial transactions and various mails and chat services over internet on laptops and mobile phones. Recently famous dating site Ashley Madison was hacked and hackers published that data including credit card details (July-August 2015). The management put 500000 $ reward for the information of hackers and the people of good social reputation committed suicide because of published data. Such kinds of events are very discouraging and restrict people in such a way so that they feel dubious to use financial transactions or chatting services specifically on ad-hoc networks. So cryptography has the responsibility to secure the transactions and various communication services. The responsibility increases manifold when the network is without infrastructure. So in this paper we present an authenticated key agreement protocols for MANETs which provides authentication as a cryptographic goal and avoids MITM (Man in the middle attack), DoS (Denial of service) etc using commitment scheme. With our proposed protocol, we wanted to achieve the security level equivalent to one time pad along with the ease of symmetric key management which involves no exponent calculations to save computational overheads.

Keywords
Authentication, Commitment, Key Agreement, Mobile Ad-hoc Networks (MANETs), Wireless Communication

1. INTRODUCTION
Need of strong security: Now days Hacktivism is in full swing. We need to rebuild the trust from the events like cracking of thousands of Ashley Madison passwords. The disclosed list by the hackers said that thousands of users use "123456" as their passwords and so many used "password" as their password. The disclosed list of using common password is even bigger. The company founded in 2002 with the appealing logo that "Life is short. Have an affair" was so lucrative and world's largest online social networking community of specific kind which serves people who are in relationship but wants to date. One can imagine the chaos by the fact that the CEO Noel Biderman steps down and many suicides are also linked to Ashley Madison leak. Texas police chief committed suicide in relation with Ashley Madison scandal as his email conversations has been leaked and the investigations are still on [1]. The reason of mentioning this is that people see these events as a security or cryptographic failure. It has long term social and economical impacts and as a result people hesitate in wireless transactions over ad-hoc connections where security is vital [2][3][4][5][6].

Commitment scheme: The term commitment is very important and specifically when it is used in development of a cryptographic protocol [7]. Making a commitment clearly means that a participating entity in a protocol is capable enough to select a value from a set or from a bit stream and commit to his choice so that it cannot change its commitment later on. This is similar to a scenario where there is a game for saddle point i.e. value of the game between two entities sender and receiver [5][8]. Sender wants to commit a bit β from the bit stream. Now Sender writes β on a paper, keeps that paper in a box and locks it with some unique mechanism say xoring of bits. Now Sender gives that box to receiver. Now here the strength of commitment is very useful; Sender can't alter its choice but has the freedom to reveal that choice at any time. A commitment scheme has two essential properties binding and revealing. In the above situation putting the paper in a box is binding and ability to disclose it anytime is revealing. Here we believe that in honest execution in an ideal commitment scheme, the receiver always accepts what a sender sends to it.

MANET characteristics and applications: Here it is of apex importance to describe MANETs because our target is to develop cryptographic protocol for it and an authenticated key agreement protocol must match with the inheriting qualities of MANETs [9][10][11][12][13][14][15]. Mobile Ad-hoc networks (MANETs) are fully distributive, infrastructure less dynamic network and have wireless mobile entities that transfer and share data with each other. MANETs do not have any fixed infrastructure and it is the salient feature which makes them very useful but at the same time making them vulnerable to various security attacks. Each entity in MANET has a wireless interface to communicate with another entity [16][17].

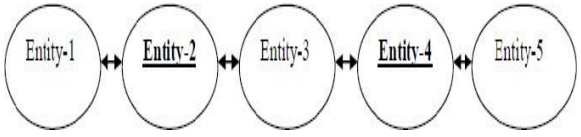

Figure-1: - Representing a MANET with five entities

Figure one represents a simple MANET with five working nodes or entities. Entity- 1 and entity -3 are not within range of each other but here entity-2 acts as an intermediate node and can be used to send packets between entity- 1 and entity-3.Similarly entity-3 and entity-5 are not directly within range of each other so entity-4 is working as an intermediate node. So entity- 2 and entity-4 acts as a router and all these five entities creates a MANET. It is important to discuss MANET characteristics which are as follows [18][19][20][21]:

Mobile entities without existing infrastructure: MANETs work without any pre defined infrastructure and there is no concept of centralized network operation and that means the

control is distributed among MANET entities. All the entities are supposed to take part and cooperate in the communication process. Since entities are mobile, they are free to move randomly so the network topology may change unpredictably. The MANET entities dynamically establish routing among themselves as they move around a range.
Multi hop routing between independent entities: As describe in the above figure-1, when a MANET entity wants to communicate with another entity which is not in its communication range directly then the communication occurs via intermediate entities. In MANET, each mobile entity is an independent entity which can function as a host and a router but at the same time dynamic topology membership may disturb the trust relationship among nodes. The trust among nodes would be disturbed if some nodes are detected as compromised or malicious.

Limited computational strength and open communication medium: While developing a cryptographic protocol for MANETs, one must keep in mind that entities have low power mobile CPUs with comparatively small memory. The wireless communication channel is open for all entities without any restriction. These wireless links have far lower capacity than well defined infrastructure networks.

Hidden terminal problem**:** It's an important issue because an entity may act as an intermediate one because two communicating nodes may not be in direct transmission range. So an entity may suffer with collision of data packets and that is always a hidden obstacle. This may leads to high transmission error. Apart from that, entities are mobile so there is always a chance of path breaks.

Computational resources: Mobile devices in networks have battery limitations. CPU processes always consume battery so a protocol for MANET must look after these issues by providing no exponent calculations and saving computational resources.

Security threats: Security is always been a challenging issue. There are multiple security issues. For example there is an involvement of intermediate nodes and there is an absence of centralized network. A MANET protocol must overcome these obstacles. An entity in MANET is free to join and leave at any time. So it's easy for an entity to behave in a selfish way. If an entity behaves maliciously then there is no mechanism to detect this hazardous situation that means lack of centralized control makes detection difficult in large size MANETs. One can develop routing algorithms and protocols in such a way so that entities are always cooperative and do not behave maliciously. It indicates that a dishonest entity can become an intermediate routing entity and the security will be in trouble. The network does not verify an entity's ID when it wants to join. So authentication is mandatory in a session cryptographic protocol and some mechanism to avoid any malicious (intruder) behavior [22][23].Some of the very important applications include [24][25][26][27]:

Military battlefield: Ad-Hoc networking will allow the military to be benefited of commonplace network technology to maintain a communication network among the soldiers, vehicles, and military information control base and various command posts.

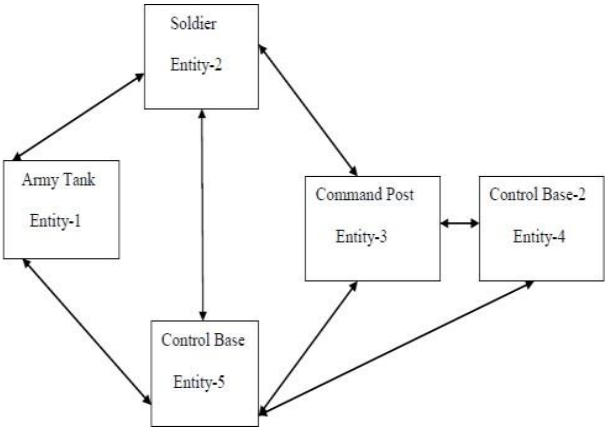

Figure-2: Representing a MANET in army battlefield

Local collaborative work: MANETs can set up an immediate sharing network to share data between entities. It is useful in conferences, lecture halls and in any premises or in domestic level where entities (residents) in an apartment share information with each other [28][29].

Emergency situation: MANETs are very useful for disaster situations and in crisis management like in earthquake where immediate communication between entities (rescue teams) is desired and no pre defined infrastructure is available. One can imagine the usefulness of MANETs by the fact that successful transmission via MANET can save many lives in a disastrous situation. So a MANET protocol is successful if it is reliable and has feature of authentication [30][31][32].

MANET security goals through cryptography**:** Developing a protocol for MANET would be successful only when it achieves important cryptographic goals and they are as follows [33][34][35][36][37]:

Confidentiality: It means to keep the content of information only for the authorized user means secrecy of the transmitted data.

Data Integrity: It deals with any unauthorized alteration of data. To achieve data integrity one must have a clear cut mechanism to detect and recognize any unauthorized access.

Authentication: It means both the parties involved in communication must find each other. There are various ways to achieve authentication. Authentication can also be subdivided into entity authentication and data origin authentication.

Non-repudiation: It makes sure that an entity cannot deny previous commitments. For example in a mutual communication process an entity should not be in the position to deny that it had agreed on a purchase of five thousand dollars.

2. PROPOSED PROTOCOL

There are two MANET entities sender (transmitter) and receiver. Sender generates random t_1 which is the time stamp. In various situations there is an essence to verify the dates of creation of documents, like in a legal registered will, it is essential to check the date of creation. Similar requirement occurs when we develop cryptographic protocols for authentication [38]. Time stamping in protocols enhances the level of security. Timestamp is mandatory when we create signed documents or session protocols for wide distribution or

for long term storage purposes. Here we are assuming that for intermediate key distribution a trusted third party i.e. a CA (certificate authority) is used. Since we want to develop a strong protocol that means even if this intermediate key distribution is compromised then also it won't affect our protocol. So we can say that the role of CA is very limited here. We are relying on the nature of the protocol and not on the CA which is a very important point. Sender has a $unique\ ID$ which may be a $device\ ID$ or a $unique\ ID$ given to Sender is denoted by $Sender_{ID}$. Sender selects a random string$A_k \in (0,1)^K$. Now Sender develops a $Code_{Sender} \leftarrow Sender_{ID} \parallel t_1 \parallel A_K$.Similarly on the other side receiver generates random t_2 which is the time stamp. Receiver has a $unique\ ID$ which may be a $device\ ID$ or a $unique\ ID$ given to receiver is denoted by $Receiver_{ID}$. Receiver selects a random string $B_k \in (0,1)^K$. Now Receiver develops a $Code_{Receiver} \leftarrow Receiver_{ID} \parallel t_2 \parallel B_K$.Now Sender develops a commitment scheme pair $(b,r) \leftarrow commitment(Code_{Sender})$ in which b is the binding parameter and r is the revealing parameter. Now Sender sends b to Receiver. In reply of this, receiver sends his $Code_{Receiver}$ to Sender. In reply Sender transmits the revealing parameter r to receiver. Now receiver is in the position to unlock the code send by sender. An ideal commitment scheme is perfectly binding and hiding. The sender has a private input that is $A_K \in (0,1)^K$and some common inputs. The commitment step generates a joint output b which is the commitment on a particular value and a specific output (r) to open it. So (b,r) is the pair. It is assumed that in an honest execution, the receiver always accepts the incoming values from sender.

Now Sender will calculate $U_{Sender} = A_K \oplus B_K$

And similarly Receiver performs $U_{Receiver} = B_K \oplus A_K$

If the two strings match then the first level authentication is successful and sender and receiver will pass further parameters to each other and if there is a mismatch in two strings we say that authentication fails.

Step-2: In the second step we have key agreement followed by bidirectional authentication means authentication for sender and receiver in such a way so that they check encryption algorithm also. Sender initiates the session that is sending $Sender\_hello$ to receiver. Now in reply of that receiver selects key K_1 and calculates $S_1 = t_1 mod\ N$ and then creates a challenge task i.e. $Challenge\ task = (t_1 \parallel ID_{rec} \parallel hash(K_1))$ and send it to sender i.e. $Reply\_challenge\_task$. The sender generates a unique current value for verification.

$$U_1 = encryption(t_1 \parallel ID_{rec} \parallel hash(K_1)$$

$$Calculate\ response = (t_2 \parallel Id_{sen} \parallel U_1)$$

Now sender sends its response i.e. t_2, ID_{sen}, U_1 to receiver. Now receiver calculates

$$U_2 = encryption(t_1 \parallel ID_{rec} \parallel hash(K_1)$$

Checks whether $U_1 = U_2$

This is called end of receiver authentication means at this stage receiver verifies the sender. Again receiver calculates

$$S_2 = t_2 mod\ N$$

$$V_1 = encryption(t_2, ID_{sen}, S_2)$$

Now receiver sends this to sender and sender calculates

$$S_2 = t_2 mod\ N$$

$$V_2 = encryption(t_2, ID_{sen}, S_2)$$

If $V_1 = V_2$ goes successful that means sender verifies the receiver. So we can say that the protocol gives bidirectional authentication. Now sender will calculate

$$secret\ key = (t_1 + t_2) mod\ N, hash\ K_1$$

Similarly receiver will calculate

$$secret\ key = (t_1 + t_2) mod\ N, hash\ K_1$$

So sender and receiver verified each other and agreed on a common secret key which is never transmitted anywhere.

3. SECURITY CONSIDERATIONS

Strong resistance to MITM**:** This is the very unique feature of our proposed protocol [39]. If a hacker (an intermediate entity in the case of MANET) has full command over the wireless communication medium then also it would not be in the authoritarian position because of the nature of commitment scheme. Suppose an intermediate entity take the responsibility of protocol initialization as a hacker with receiver and pretends to be sender. Intermediate entity will send his commitment value b^* to receiver which is the commitment of calculating the random string i.e.I_K where $I_K \in (0,1)^K$and $Code_{Int\ entity} \leftarrow Int\ entity_{ID} \parallel t^* \parallel I_K$and send it to receiver. The receiver will send his code i.e. $Code_{Receiver}$ to hacker. Now hacker modifies the incoming message from receiver and sends it to sender. In reply of that sender will send (b,r) pair in which b is the commitment value which reveals no information about $Code_{Sender}$ but committed to a particular value only. So apart from all hacking effort, when it comes to the authentication stage of a protocol which is nothing but the calculation of U_{Sender} and $U_{Receiver}$, the two bit streams will not match. As a result sender and receiver do not communicate further and will not exchange further protocols parameters and saves their computational overhead and time. All the hacking efforts of hacker go in vain and the communication flow remains safe.

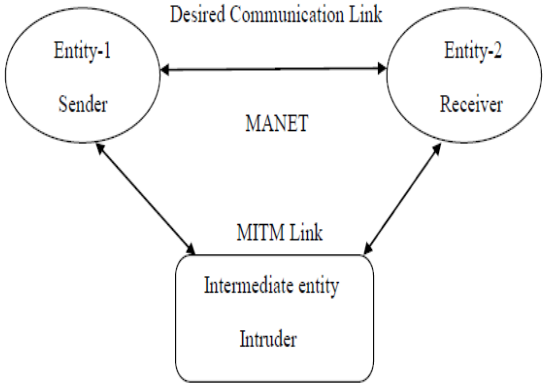

Figure-3: Representing MITM link

No collision protocol: The commitment scheme (b, r) is an ideal commitment scheme and that is our basic assumption. It means that the commitment value b is unique for $Code_{Sender}$ in such a way so that $b^* = b$ is never possible until $Code_{Sender}$ is not known. The same security assumption we have for r also.

Possibility of successful hacking effort (Initial Brute Force Attack): The single chance of Intermediate entity's success is when Sender and hacker both generate a same random string (say K bits each). So the probability of success will be $P_{Int\ entity} = 2^{-K}$.If we select $K = 25$ bits then $P_{Int\ entity} = 2^{-25}$ and that is equal to $2.98 * 10^{-8}$. Since $P_{Int\ entity}$ is negligible for 25 bit size then there is no question of discussing it and even bigger bit size will enhance the security level that in turn reduces the probability of success of intermediate entity.

Denial of service attack: There is no chance of Denial of Service attack because our protocol has the special property of commitment scheme which has binding and hiding property. The sender can't deny that it has not initiated the communication or can't deny the previously made commitments.

4. CONCLUSION

MANETs are one of the most emerging areas. Now a days we chat, email and do a lot of financial transactions by our mobile phones [40]. MANETs are very lucrative because of its ease of use as they don't have any fixed infrastructure. Our protocol is very easy to implement and it does not have any exponent calculation keeping the fact in mind that MANET entities are mobile with limited CPU strength. To achieve security strength of one time pad is really difficult and the protocol provides the same.

5. FUTURE SCOPE

The future scope of the protocol is very rich because it can be implemented in ad-hoc networks operating at various important situations like military battlefield or in specific customized services like electronic health record systems where authentication and key agreement plays vital role. The protocols provide simplicity with mathematical solidity so that they can be applied with other wireless communication scenarios like RIP (Routing information protocol) and OSPF (Open shortest path first) which are the examples of distance vector routing and link state routing respectively.

6. REFERENCES

[1] Mail online-News, Two suicides are linked to Ashley Madison leak: Texas police chief takes his own life just days after his email is leaked in cheating website hack.www.dailymail.co.uk/news/article-3208907/The-Ashley-Madison-suicide-Texas-police-chief-takes-life-just-days-email-leaked-cheating-website-hack.html

[2] Y.Amir, Y.Kim, C.N.Rotaru, J.L.Schultz, J.Stanton, G.Tsudik, Secure group communication using robust contributory key agreement, IEEE transactions on parallel and distributed systems, volume 15, number 4, 2004.

[3] A.Asadi, V.Mancuso, Energy efficient opportunistic uplink packet forwarding in hybrid wireless networks, Proceedings of the fourth international conference on future energy systems, Berkeley, California, USA, 2013, 261-262.

[4] D.Balfanz, D.K.Smetters, P.Stewart, H.C.Wong, Talking to strangers: Authentication in ad-hoc wireless networks, In symposium on network and distributed systems security, San Diego, California, USA, 2002.

[5] M.Bellare, P.Rogaway, Entity authentication and key distribution, Advances in cryptology, Crypto'93, Proceedings Springer-Verlag, 1993, 232-249.

[6] X.Lin, R.Lu, H.Zhu, P.H.Ho, X.Shen, Z.Cao, An anonymous secure routing protocol with authenticated key exchange for wireless ad-hoc networks, ICC-2007, 1247- 1253.

[7] V.Shukla, N.Srivastava, A.Chaturvedi, A bit commitment signcryption protocol for wireless transport layer security (WTLS), IEEE Uttar Pradesh section international conference on electrical, computer and electronics engineering (UPCON), 2016, 83-86.

[8] V.Shukla, A.Chaturvedi, N.Srivastava, A new secure authenticated key agreement scheme for wireless(mobile) communication in an EHR system using cryptography, Communications on applied electronics(CAE), Foundation of computer science (FCS), New York, USA, volume 3, number 3, 2015, 16-21.

[9] I.B.Damgard, T.P.Pedersen, B.Pfitzmann, Statistical secrecy and multibit commitments, IEEE transactions on information theory, volume 44, issue 3, 1998, 1143-1151.

[10] E.Bresson, O.Chevassut, A.Essiari, D.Pointcheval, Mutual authentication and group key agreement for low-power mobile devices, The fifth IFIP-TC6 international conference on mobile and wireless communication networks, 2003, Singapore, 59-62.

[11] M.Cagalj, S.Capkun, J.P.Hubaux, Key agreement in peer-to-peer wireless networks, Proceedings of the IEEE, volume 94, number 2, 2006.

[12] K.Sanzgiri, B.Dahill, B.N.Levine, C.Shields, E.M.B.Royer, A secure routing protocol for ad-hoc networks, Proceedings of the 10th IEEE international conference on network protocols (ICNP), 2002.

[13] M.Wazid, R.K.Singh, R.H.Goudar, A survey of attacks happened at different layers of mobile ad-hoc network & some available detection techniques, Proceedings published by international journal of computer applications (IJCA), international conference on computer communication and networks CSI-COMNET, 2011.

[14] A.Weimerskirch, D.Westhoff, Identity certified authentication for ad-hoc networks, Proceedings of the first ACM workshop on security of ad-hoc and sensor networks, 2003, USA, 33-40.

[15] L.Zhou, Z.J.Haas, Securing ad-hoc networks, IEEE network, special issue on network security, 1993, 24-30.

[16] S.Zhu, S.Xu, S.Setia, S.Jajodia, LHAP: A light weight hop-by-hop authentication protocol for ad-hoc networks, Proceedings of the 23rd international conference on distributed computing systems workshops (ICDCSW), 2003.

[17] H.Deng, W.Li, D.P.Agrawal, Routing security in wireless ad-hoc networks, IEEE communication magazine, volume 40, issue 10, 2002, 70-75.

[18] W.Du, J.Deng, Y.S.Han, P.K.Varshney, A pair wise key pre-distribution scheme for wireless sensor networks, Proceedings of the 10th ACM conference on computer and communications security, 2003, 42-51.

[19] L.Eschenauer, V.D.Gligor, A key management scheme for distributed sensor networks, Proceedings of the 9th ACM conference on computer and communications security, 2002, 41-47.

[20] G.Foder, E.Dahlman, G.Mildh, S.Parkvall, N.Reider, G.Miklos, Z.Turanyi, Design aspects of network assisted device-to-device communications, IEEE communication magazine, volume 50, issue 3, 2012.

[21] O.H.Younis, S.E.Essa, A.E.Sayed, A survey on security attacks/defenses in mobile ad-hoc networks, Communications on applied electronics (CAE), foundation of computer science(FCS), New York, USA, volume 6, number 10, 2017.

[22] N.Goyal, A.Gaba, A review over MANET-issues and challenges, international journal of research in management & computer applications, volume 2, issue 4, 2013, 16-28.

[23] A.Chaturvedi, N.Srivastava, V.Shukla, A secure wireless communication protocol using Diffie-Hellman key exchange, International journal of computer applications, volume 126, number 5, 2015, 35-38.

[24] A.Chaturvedi, N.Srivastava, V.Shukla, S.P.Tripathi, M.K.Misra, A secure zero knowledge authentication protocol for wireless (mobile) ad-hoc networks, International journal of computer applications, volume 128, number 2, 2015, 36-39.

[25] S.Mohseni, R.Hassan, A.Patel, R.Razali, Comparative review study of reactive and proactive routing protocols in MANETs, 4th IEEE international conference on digital ecosystems and technologies (DEST), 2010, 304-309.

[26] C.Perkins, E.B.Royer, S.Das, Ad-hoc on demand distance vector(AODV) routing, RFC, 2003 http://dl.acm.org/citation.cfm?id=RFC3561

[27] A.A.Pirzada, C.McDonald, Kerberos assisted authentication in mobile ad-hoc networks, In proceedings of the 27th Australasian conference on computer science, volume 26, 2004, 41-46.

[28] M.T.Refaei, V.Srivastava, L.Dasilva, M.Eltoweissy, A reputation-based mechanism for isolating selfish nodes in ad- hoc networks, The second annual international conference on mobile and ubiquitous systems: networking and services, San Diego, USA, 2005.

[29] F.H.Tseng, L.D.Chou, H.C.Chao, A survey of black hole attacks in wireless mobile ad-hoc networks, Human-centric computing and information sciences, Springer, volume 1, issue 4, 2011, 1-16.

[30] L.Venkatraman, D.P.Agrawal, A novel authentication scheme for ad-hoc networks, IEEE wireless communication and networking conference, Chicago, USA, 2000, 1268-1273.

[31] D.C.Mur, A.G.Saavedra, P.Serrano, Device to device communications with Wi-Fi direct: overview and experimentation, IEEE wireless communications, volume 20, Issue 3, 2013, 96-104.

[32] S.Sarika, A.Pravin, A.Vijayakumar, K.Selvamani, Security issues in mobile ad-hoc networks, 2nd international conference on intelligent computing, communication & convergence (ICCC), Procedia computer science 92,Elsevier, 2016, 329-335.

[33] R.J.Sutton, Secure communication: Applications and management, third edition, John Wiley & Sons, 2002.

[34] B.A.Forouzan, Cryptography & network security, Tata McGraw-Hill, New York, 2007.

[35] L.Law, A.Menezes, M.Qu, J.Solinas, S.Vanstone, An efficient protocol for authenticated key agreement, Design codes and cryptography, volume 28, issue 2, 2003, 119-134.

[36] W.Mao, Modern cryptography: Theory and practice, Prentice Hall PTR, New Jersy, USA, 2003.

[37] A.J.Menezes, P.C.V.Oorschot, S.A.Vanstone, Handbook of applied cryptography, fifth edition, CRC press INC, USA, 2001.

[38] A.J.Menezes, M.Qu, S.A.Vanstone, Key agreement and the need for authentication, presentation at PKS'95, Toronto, Canada, 1995.

[39] P.Burkholder, SSL Man in the middle attack, Sans institute, 2002. https://www.sans.org/readingroom/whitepapers/threats/sslman-in-the-middle-attacks-480.

[40] S.I.Siddiqui, S.Jabeen, M.Mumtaz, whether cell phone is a necessary or a luxurious item, middle east journal of scientific research, 2014, 61-65.