A Distributed Session Initiation Protocol Solution for Mobile Ad Hoc Networks Using Elliptic Curve Cryptography

A.F. Aburumman, W.J. Seo, A. Yang and K-K. R. Choo

[a] *Information Assurance Research Group, School of Information Technology and Mathematical Sciences,*
University of South Australia, South Australia
Email: seowy002@mymail.unisa.edu.au

Abstract: Mobile devices (e.g. iPhones and iPads) are on the top of technology pyramid now days. Mobile Ad hoc Networks (MANETs) is one of the hot and challenging topics in the field of computer and telecommunication research. What make MANETs distinctive are the specifications (i.e. infrastructure-less and self-configuring) that provide an autonomous way to connect mobile devices. One of the current and most challenging areas is the implementation of Voice over IP (VoIP) services over MANETs. Such implementation requires a well-structured solution considering all factors, such as voice protocol, routing protocol and security mechanism, to form a solid solution for such implementation. In this paper, we extend our previous solutions published in 2013 and 2014 of adapting the widely used Session Initiation Protocol (SIP) (a signaling protocol used to establish, manage and tear a VoIP session) over MANETs by enhancing the solution with a security suite using the Elliptic Curve Cryptography (ECC). Our proposed solution provides an enhanced security mechanism for such implementation with relatively low cost on the network to form the underlying model of adapting SIP service over MANETs. The proposed solution is simulated under different conditions and scenarios using various metrics and compared with our previous works from 2013 and 2014.

Keywords: *Mobile Ad hoc Networks (MANETs), Session Initiation Protocol (SIP), Voice over IP (VoIP), ECC*

1. INTRODUCTION

Mobile devices are the pivot of technology for the tech-savvy generations of these days. Mobile applications and software serve as keys to enter different dimensions of services. VoIP is one of the most important services in mobile devices(Keromytis, 2011).

Due to the increasing popularity of mobile devices, an application to be used in case of emergency situation (out-of-range, natural disasters) is critical. Mobile Ad hoc Networks (MANETs) could be the key to this dimension.

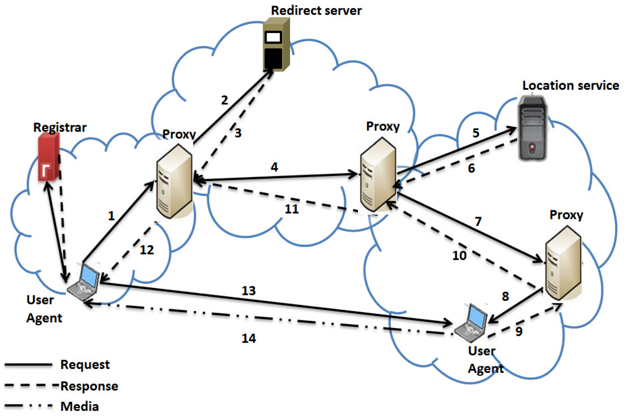

Figure 1. SIP Overly Network architecture.

Adapting VoIP protocols over MANETS is the way to form such solution. Consequently, the modification of existing protocol such as Session Initiation Protocol (SIP) to be utilized in a peer-to-peer (P2P) communication environment, and without compromising on availability and security is essential (El Sawda and Urien, 2006).

In this paper, we propose a SIP solution for MANET equipped with ECC suite as an extension of our previous works in Aburumman et al. in 2013 and 2014.

2. BACKGROUND: OVERVIEW AND RELATED WORK

2.1 Brief overview of SIP

SIP is an application layer protocol developed by the IETF responsible of initiating, managing and terminating the multimedia sessions. SIP builds an overlay network on top of regular IP-network by using a set of several components as shown in figure 1. (Rosenberg, 2002)

SIP components consist of endpoint agents to interact with the user called User Agents (UA), various functioning servers to communicate with each other or with the UA providing service called Proxy, Registrar and Redirect servers and gateways to translate SIP into other protocols which is usually used to connect SIP networks to the PSTN (Rosenberg, 2002).

The protocol also contain two databases to store information about the service, one is called Location Service database of those who have registered through a SIP server, and where they are located, and the other is an Address-of-Record database that holds SIP User Id and relevant contact information.

2.2 Related Work

As found in literature very few papers have touch based on issue of implementing a secure SIP over MANETS.

Fessi et al. (2010) present security mechanisms called Privacy-Preserving peer-to-peer SIP (Pr2-P2PSIP). The mechanism is designed to overcome the privacy issues in P2PSIP by providing a location and social interaction privacy with a tunnel length of three for inbound tunnels and two for outbound tunnels. The mechanism deploys ECC as part of the solution. The authors claim that such deployment does not produce a significant overhead on the network (Fessi, 2010).

More recent in 2012, Alshingiti proposed an enhanced security mechanism for SIP over ad hoc networks. In her research, an extension to the SIP header was introduced to enhance its security for ad hoc networks. This is done by combining Cryptographically Generated Addresses (CGA) with the social network paradigm to provide authentication and message integrity (Alshingiti, 2012).

Another secure cluster-based SIP service was introduced by Abdullah et al. in 2013. The method could protect the SIP service from attacks that aims to reduce service function in SIP network which is also known as the calls success ratio. The result of their work minimized the disadvantages of centralized approaches. Such method also reduces the overhead which exist in the distributed models.

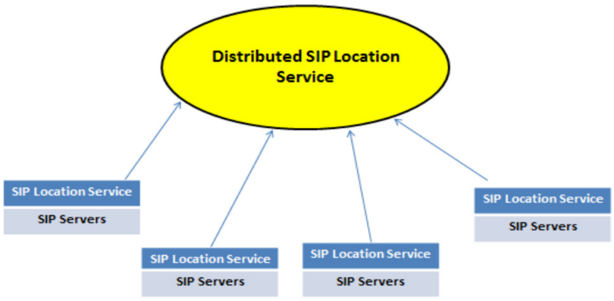

Figure 2. Distributed SIP Location Service.

3. SYSTEM MODEL AND DESIGN

In this section, we briefly explain the proposed solution from Aburumman et al. 2013 and 2014 to help magnifying the equipped security suite using ECC as part of the solution. We then show the effect of such implementation on the network by simulating the proposed solution.

3.1 Brief Recap of our Previous Solutions

The solution from previous research has illustrated that each node in the network is equipped with the capability to act as SIP servers with activated functionality that is required in the MANET. Each node shares a distributed location service of the nodes interested in the service as shown in figure 2. The location service could be updated in different methods (Aburumman, 2013).

As presented in the design during 2013 and 2014, the first node to initiate during the startup the service will be the Primary Server (PS). PS will select a Backup Server (BS) from the interested nodes in the server to keep the network up and updated as required. The selection criteria of the nodes to be acting as a server in the network is based on the trust level equations and feedback form the network (Power, Resources, and stability).

Once initiated, the interested nodes join the network and privileged nodes with capability to serve the network will take roles administrating the network and keeping the network alive and updated. In case if any of the acting servers are down or leaving for any reason (low power, mobility, etc...), an election based on the aforementioned criteria will take a place recovering the missing server. The detailed of the design was published in Aburumman et al. 2013 and 2014.

3.2 Proposed ECC suite for SIP Over MANET

In this section, ECC suite will be extended to the previous work from as described in previous section.

I. Notations of ID-based Authentication Group Key Exchange Protocol with Pairing–Free

S: Servers including Ps (primary servers) and Bs (backup servers) **C**: Clients who is joining or joined the network. **d**: Private key. **P**: Public key. **r**: Temporary private key. **R**: Temporary public key.	**K**: Session Key **a,b** : $a, b \in f_q$, are the parameters of the elliptic curve E on Fq where elliptic function is $y^2 = x^3 + ax + b$. **G**: The base point of elliptic curve. Order of G is prime number that G = (xG; yG). **ID**: Identification of participants. **H()**: Hash Function.

II. Key Establishment Process

In this protocol, the group of servers including Ps and Bs are being denoted as $S_1,\ S_2,\ S_3, \dots S_n$, and a group of clients are being denoted as $C_1,\ C_2,\ C_3, \dots C_n$.

The servers will generate their private key using: $d_{S_i} \in [1, n-1]$ and compute the corresponding public key using: $P_{S_i} = [d_{S_i}]G = (x_{S_i}, y_{S_i})$.

Clients will perform similar process to acquire a private key using: $d_{C_i} \in [1, n-1]$ and compute the corresponding public key using: $P_{C_i} = [d_{C_i}]G = (x_{C_i}, y_{C_i})$. Both servers and clients will compute their identification using: $ID_{S_i} = H(x_G||y_G||a||b||x_{S_i}||y_{S_i})$ and $ID_{C_i} = H(x_G||y_G||a||b||x_{C_i}||y_{C_i})$ respectively, before sending their information such as: $P_{S_i}, P_{C_i}, ID_{S_i}, ID_{C_i}$ to others. The publish hash function used are $H_1()$ *and* $H_2()$.

In this stage, group session key between servers and clients will be generated and exchange,

Round 1: Temporary Public Key Establishment

The Servers (S) will generate temporary private key which will be used for temporary public key

1. Randomly select a temporary private key using: $r_{S_i} \in [1, n-1]$,
2. And compute $t_{S_i} = (d_{S_i} \cdot r_{S_i})$*mod n*, then compute the temporary public key using: $R_{S_i} = [r_{S_i}]G = (x_{Sn}, y_{Sn})$,

Similarly, the Clients (C) will generate temporary private key which will be used for temporary public key

3. Randomly select a temporary private key using: $r_{C_i} \in [1, n-1]$,
4. And compute $t_{C_i} = (d_{C_i} \cdot r_{C_i})$*mod n*, then compute the temporary public key using: $R_{C_i} = [r_{C_i}]G = (x_{Cn}, y_{cn})$,
5. Broadcasting the temporary public key R_{S_i}, R_{C_i} to others which are already in the network.

Round 2: Key Establishment

1. S will compute U using:
   $U_{S_i} = [t_{S_i}] \cdot (\Pi_{i=1}^{n} x_{Sn} x_{Cn}, \Pi_{i=1}^{n} y_{Sn} y_{Cn}) + d_{S_i} \cdot (\Pi_{i=1}^{n} x_{S_i} x_{C_i}, \Pi_{i=1}^{n} y_{S_i} y_{C_i}) = (x_{S_U}, y_{S_U})$,
   U is the verified using: $U \overset{?}{=} (0,0)$ but abort if the verification fails. Otherwise, the server will compute the session key which is: $K = H_1(x_{S_U} \parallel y_{S_U} \parallel ID_{S_1} \parallel ID_{S_2} \parallel \cdots \parallel ID_{S_n} \parallel ID_{C_1} \parallel ID_{C_2} \parallel \cdots \parallel ID_{C_n})$
2. Likewise C will compute U using:
   $U_{C_i} = [t_{C_i}] \cdot (\Pi_{i=1}^{n} x_{Sn} x_{Cn}, \Pi_{i=1}^{n} y_{Sn} y_{Cn}) + d_{C_i} \cdot (\Pi_{i=1}^{n} x_{S_i} x_{C_i}, \Pi_{i=1}^{n} y_{S_i} y_{C_i}) = (x_{C_U}, y_{C_U})$,
   U is verified using: $U \overset{?}{=} (0,0)$ but abort if the verification fails. Otherwise, the client will compute the session key which is: $K = H_1(x_{C_U} \parallel y_{C_U} \parallel ID_{S_1} \parallel ID_{S_2} \parallel \cdots \parallel ID_{S_n} \parallel ID_{C_1} \parallel ID_{C_2} \parallel \cdots \parallel ID_{C_n})$

Therefore the Group Key establishment is:

For servers:

$$\mathrm{K} = \mathrm{H}_1(\mathrm{x}_{\mathrm{S_U}} \parallel \mathrm{y}_{\mathrm{S_U}} \parallel \mathrm{ID}_{\mathrm{s}_1} \parallel \mathrm{ID}_{\mathrm{s}_2} \parallel \cdots \parallel \mathrm{ID}_{\mathrm{s_n}} \parallel \mathrm{ID}_{\mathrm{C}_1} \parallel \mathrm{ID}_{\mathrm{C}_2} \parallel \cdots \parallel \mathrm{ID}_{\mathrm{C_n}})$$

For clients

$$K = H_1(x_{C_U} \parallel y_{C_U} \parallel ID_{S_1} \parallel ID_{S_2} \parallel \cdots \parallel ID_{S_n} \parallel ID_{C_1} \parallel ID_{C_2} \parallel \cdots \parallel ID_{C_n})$$

III. Join and Leave The Network

Join Protocol

Whenever a new client is joining the network, the following processes will occur after authentication and authorization of the primary servers:

1. New client is being represented as C_J (J > n).
2. C_J will generate its own private key and temporary private key using $d_{C_J} \in [1, n-1]$ and $r_{C_J} \in [1, n-1]$, respectively.
3. And then C_J will compute its public key using: $P_{C_J} = \left[d_{C_J}\right]G = \left(x_{C_J}, y_{C_J}\right)$, and its own t using: $t_{C_J} = (d_{C_J} \cdot r_{C_J})\boldsymbol{mod n}$, and its own identification using: $ID_{C_J} = H(x_G||y_G||a||b||x_{C_j}||y_{C_j})$, as well as its own temporary public key using $R_{C_J} = \left[r_{C_J}\right]G = (x_{Cj}, y_{Cj})$,
4. Then C_J will broadcast its information such as $P_{S_J}, R_{C_J}, ID_{C_J}$ to others in the network.

When S and Cs receive $P_{C_J}, R_{C_J}, ID_{C_J}$, they will send P, R, ID to C_J. Then compute a new session key within the network.

Upon accepting the information from C_J , on the server side, S will compute a new session key U using:

$U_{S_i} = \left[t_{S_i}\right] \cdot \left(\Pi_{i=1}^{n} x_{Sn} x_{Cn} x_{Cj}, \Pi_{i=1}^{n} y_{Sn} y_{Cn} y_{Cj}\right) + d_{S_i} \cdot \left(\Pi_{i=1}^{n} x_{S_i} x_{C_i} x_{C_j}, \Pi_{i=1}^{n} y_{S_i} y_{C_i} y_{C_j}\right) = (x_{S_U}, y_{S_U})$U is then verified using: $U \overset{?}{=} (0,0)$ but abort if the verification fails. Otherwise, the server will compute the Group Session key which is: $K = H_1(x_{S_U} \parallel y_{S_U} \parallel ID_{S_1} \parallel ID_{S_2} || \ldots \parallel ID_{S_n} \parallel ID_{C_1} \parallel ID_{C_2} \parallel \cdots \parallel ID_{C_n} \parallel ID_{C_J})$

The rest of the clients will also compute a new session key using:

$U_{C_i} = \left[t_{C_i}\right] \cdot \left(\Pi_{i=1}^{n} x_{Sn} x_{Cn} x_{Cj}, \Pi_{i=1}^{n} y_{Sn} y_{Cn} y_{Cj}\right) + d_{C_i} \cdot \left(\Pi_{i=1}^{n} x_{S_i} x_{C_i} x_{C_j}, \Pi_{i=1}^{n} y_{S_i} y_{C_i} y_{C_j}\right) = (x_{C_U}, y_{C_U})$Likewise, U is then verified using: $U \overset{?}{=} (0,0)$ but abort if the certification fails. Otherwise, the client will compute the Group Session which is: $K = H_1(x_{C_U} \parallel y_{C_U} \parallel ID_{S_1} \parallel ID_{S_2} \parallel \cdots \parallel ID_{S_n} \parallel ID_{C_1} \parallel ID_{C_2} \parallel \cdots \parallel ID_{C_n} \parallel ID_{C_J})$

Leave Protocol

When a client is leaving the MANET, the following process will occur:

1. If client C_j (1<j<n) wants to leave the MANET, C_j will send leave information to server S.
2. Then rest of the servers and clients will react as below:

S will compute a new U using:

$U_{S_i} = \left[t_{S_i}\right] \cdot \left(\Pi_{i=1}^{n} x_{Sn} x_{Cn} / x_{Cj}, \Pi_{i=1}^{n} y_{Sn} y_{Cn} / y_{Cj}\right) + d_{S_i} \cdot \left(\Pi_{i=1}^{n} x_{S_i} x_{C_i} / x_{C_j}, \Pi_{i=1}^{n} y_{S_i} y_{C_i} / y_{C_j}\right) = (x_{S_U}, y_{S_U})$U is then verified using $U \overset{?}{=} (0,0)$ but abort if the verification fails. Otherwise, the client will compute a new session key using: $K = H_1(x_{S_U} \parallel y_{S_U} \parallel ID_{S_1} \parallel ID_{S_2} \parallel \cdots \parallel ID_{S_n} \parallel ID_{C_1} \parallel ID_{C_2} \parallel \cdots \parallel \cancel{ID_{C_J}} \parallel \cdots \parallel ID_{C_n})$

Similarly C will compute a new U using:

$U_{C_i} = \left[t_{C_i}\right] \cdot \left(\Pi_{i=1}^{n} x_{Sn} x_{Cn} / y_{Cj}, \Pi_{i=1}^{n} y_{Sn} y_{Cn} / y_{Cj}\right) + d_{C_i} \cdot \left(\Pi_{i=1}^{n} x_{S_i} x_{C_i} / x_{C_j}, \Pi_{i=1}^{n} y_{S_i} y_{C_i} / y_{C_j}\right) = (x_{C_U}, y_{C_U})$U is then verified using $U \overset{?}{=} (0,0)$ but abort if the verification fails. Otherwise, the client will compute a new session key using: $K = H_1(x_{C_U} \parallel$

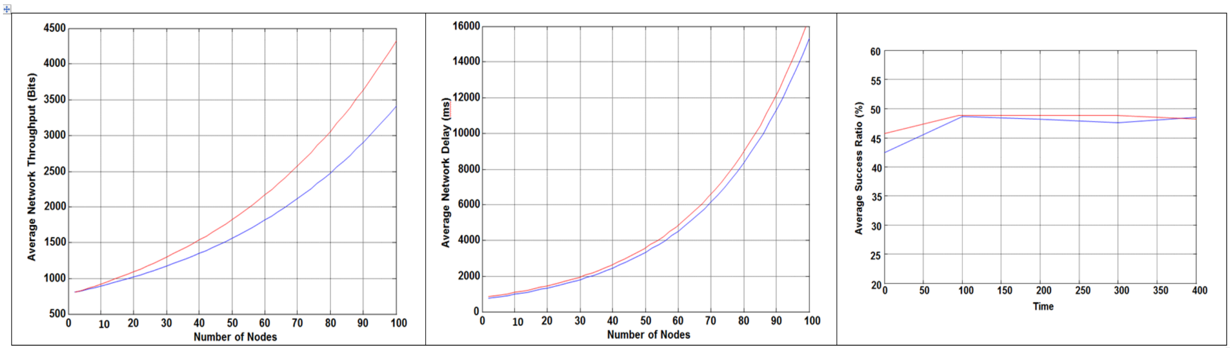

Figure 3. (a) Trust Network Throughput vs. Number of Nodes. (b) Average Network Delay vs. Number of Nodes. (c) Average Success Ratio vs. Number of nodes.

$$y_{C_U} \parallel ID_{s_1} \parallel ID_{s_2} \parallel \cdots \parallel ID_{s_n} \parallel ID_{C_1} \parallel ID_{C_2} \parallel \cdots \parallel \cancel{ID_{C_j}} \parallel \cdots \parallel ID_{C_n})$$

The implementation of ECC provided an enhanced solution for implementing SIP over MANET . Such implantation is considers the separation of providing different levels of security for the servers versus clients functionality based on the role that the node is playing. The overall implementation added a relatively reasonable overheard while overcoming significant security challenges.

In the next section, the implementation is simulated and examined using different scenarios' changing the parameters of the network to provide more realistic application of such implementation.

4. EXPERIMENTS AND RESULTS ANALYSIS

The proposed mechanism was simulated and Figure 3 shows the simulation's results evaluated based on the following evaluation metrics:
Throughput: The rate of successful messages over the communication channels.
Success Ratio: Measures the number of success invitations to the intended recipient over time.
Stability: Shows the consistency with increasing number of nodes and its effect on the service request time.
Network Delay: The period of time taken to transfer the data across the network.

The parameter values used in the evaluation are as follow:
Time: The amount of time in seconds for the running of the network. For each second run-time, the simulation time may not be equivalent to one second in real networks.

Number of Nodes: Number of nodes in the simulation environment.

Figure 3(a) depicts the effect of the increasing in the number of nodes on the average network throughput. The blue represent the results from the previous solution, compared with the red which are the new proposed solution that integrate ECC suite. Apparently, there is a slight increase from the blue curves which is justified by the added security value to the solution. As shown in the figure, the average throughput of the new solution is slightly higher, but it's relatively low as it's inherited from the low cost of embedding ECC into the solution (Yang, 2014).

Figure 3(b) illustrates the effect of the increasing in the number of nodes on the average network delay. The noticeable difference between both curves which reflects the average delay is negligible. Again, this is due to the low cost of ECC implementation.

Figure 3(c) studies the stability of proposed mechanism in terms of success ratio for all nodes against the increase in the number of nodes. It can be observed that the success ratio stabilizes with the increase in the number of nodes. This suggests that the proposed mechanism is still stable and scalable with the increase of the network size.

5. CONCLUSIONS AND FUTURE WORK

This paper proposes a new extended security mechanism to our previous works from Aburumman 2013 and 2014 using ECC. The mechanism provides a higher security scheme while maintaining a stable and scalable SIP services for MANETS. This solution comes with slightly higher average throughput which is considerably rational, in comparison with the added value of having a better security scheme embedded to acquire better availability and privacy to the provided service. Moreover, the solution almost maintains the same average network delay and success ratio.

Future work includes examining ways of having a new integrated solution that overcome more security threats and produce more scalable system. This could be achieved by injecting different security threats to the network and analyze the overall network performance to mitigate threats. It could also propose more adaptive SIP protocol with more efficient routing protocol to produce better scalability, stability and availability to provide SIP service over MANETs.

REFERENCES

Abdullah, L., Almomani, I., & Aburumman, A. (2013) Secure cluster-based SIP service over Ad hoc networks. In Proceedings of IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT 2013), pp. 1-7, IEEE 2013

Aburumman, A., Choo, K-K. R., and Lee, I. (2013). Nomination-based session initiation protocol service for mobile ad hoc networks, Gaertner, P., Bowden, F., Piantadosi, J. and Mobbs, K. (eds) 22nd National Conference of the Australian Society for Operations Research (ASOR 2013). The Australian Society for Operations Research, Adelaide, pp. 149–155, 1–6 December 2013

Aburumman, A., and Choo, K-K. R (2014). A Domain-Based Multi-cluster SIP Solution for Mobile Ad Hoc Network, Applications and Techniques in Cyber Security, Beijing.

Alshingiti, M. (2012). Security Enhancement for SIP in Ad Hoc Networks (Doctoral dissertation, CARLETON UNIVERSITY Ottawa).

El Sawda, S., and Urien, P. (2006). SIP Security Attacks and Solutions: A state-of-the-art review. In Information and Communication Technologies, 2006. ICTTA'06. 2nd (Vol. 2, pp. 3187-3191). IEEE.

Fessi, A., Evans, N., Niedermayer, H., and Holz, R. (2010). Pr2-P2PSIP: privacy preserving P2P signaling for VoIP and IM. In Principles, Systems and Applications of IP Telecommunications (pp. 134-145). ACM.

Keromytis, A. D. (2012). A comprehensive survey of voice over IP security research. Communications Surveys & Tutorials, IEEE, 14(2), 514-537.

Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and Schooler, E. (2002). SIP: session initiation protocol (No. RFC 3261).

Yang, A., Nam, J., Kim, M., & Choo, K. K. R. (2014). Provably-Secure (Chinese Government) SM2 and Simplified SM2 Key Exchange Protocols. The Scientific World Journal, 2014.