Nomination-based Session Initiation Protocol Service for Mobile Ad Hoc Networks

Ala' Aburumman [a], Kim-Kwang Raymond Choo [a] and Ivan Lee [a]

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

Abstract: With the increasingly popularity of mobile devices (e.g. iPhones and iPads), Mobile Ad hoc Networks (MANETs) has emerged as one of the topical research areas in recent years. The special characteristics of MANETs (i.e. infrastructure-less and self-configuring) provide a flexible way of connecting mobile devices. Due to the inherent characteristics of MANETs (e.g. self-configuration of IP addresses), implementing Voice over IP (VoIP) services over MANETs remains an ongoing research challenge. In this paper, we demonstrate how we can adapt the widely used Session Initiation Protocol (SIP) (a signaling protocol used to establish, manage and tear a VoIP session) over MANETs using the Nomination-based mechanism. Our proposed solution employs two security mechanisms to form the underlying model of adapting SIP service over MANETs. We then simulated the setup under different conditions and evaluated the results using various metrics (e.g. Trust Level, Proxy Server (PS) Load, Network Delay, Success Ratio, Network Management Packets, Scalability, and Stability).

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

1. INTRODUCTION

Wireless devices play an important role in our daily communications, supporting applications such as Radio Frequency Identification (RFID) and Voice over IP (VoIP). The latter can be used to deliver voice and video over the internet – i.e. Internet Protocol (IP) networks, instead of the Public Switched Telephone Network (PSTN). In IP-based network, the most widely known signaling protocols are the: H.323-defined by the ITU, and the Session Initiation Protocol (SIP) - defined by the IETF. In recent years, SIP is becoming more widely used (as compared to H.323) due to its flexibility and relative simplicity (Keromytis, 2011).

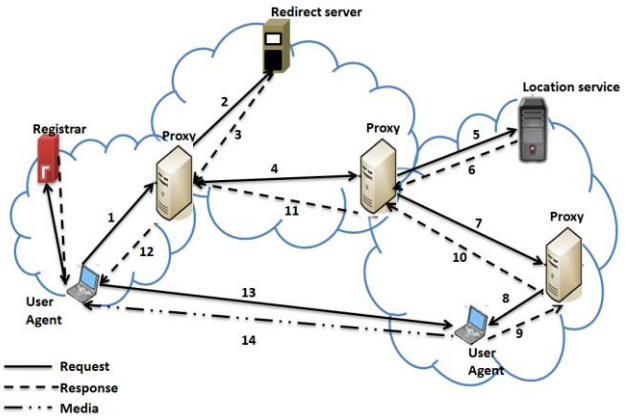

Figure 1. SIP Overly Network architecture

Due to the increasing popularity of 802.11/Wi-Fi enabled devices with more powerful capabilities such as smart mobile devices, Ad hoc networks are used to support various applications that run on such devices. One such application is inexpensive communication using VoIP application on Wi-Fi-enabled devices. However, the pre-infrastructure networks are always a way to charge you and control your communication with others people. The implementation of voice protocol over MANETs would also be a good option to communicate with others in case you don't have network coverage in any area.

Therefore, it is necessary that VoIP signaling services are modified in order to be used in decentralized infrastructure-less networks. To do so, tone could modify existing Session Initiation Protocol (SIP) components to be utilized in a peer-to-peer (P2P) communication environment, and without compromising on availability, flexible design and accepted call ratio (El Sawda & Urien, 2006). This will lead to the ability to communicate free of cost as no infrastructure is involved. It also means you are never "Out of Range" as long as people exist around you.

In this paper, we propose a nomination-based solution to adapt SIP for MANET that provides secure P2P communications.

2. BACKGROUND: OVERVIEW AND RELATED WORK

2.1. Brief overview of SIP

VoIP application enables voice and video communications to take place over an IP network instead of traditional analog systems. VoIP is a suite of protocols and methodologies and transmission technologies. For example, Session Initiation Protocol (SIP) is used for signaling; Session Description Protocol (SDP) for describing techniques used in media transfer, and Real-Time Protocol (RTP) is used for media packets transfer. The functional building block for multimedia application is the signaling protocol. In IP-based network the most known signaling protocols are: H.323 and SIP (Kumar, 2006).

SIP, an application layer developed by the IETF, is defined in RFC3261 (Rosenberg et al., 2002). It is initially designed to accommodate multimedia sessions such as VoIP. Fundamentally, SIP is used for initiating, managing and terminating the multimedia sessions for voice and video across packet switched networks. Usually SIP sessions involve one or more participants on SIP-enabled devices (Sparks, 2007). SIP builds an overlay network on top of regular IP-network by using a set of several entities communicated via SIP messages. The three main SIP Entities are:

User Agents (UA): SIP endpoint interacts with the user.

Servers (Proxy, Registrar and Redirect): they communicate with each other or with the UA providing service.

Gateways: translate SIP into other protocols. Usually used to connect SIP networks to the PSTN(Rosenberg et al., 2002; Sparks, 2007). Typical SIP overlay network architecture is illustrated in **Error! Reference source not found.**.

Location service (LS): is a component to keep a database of those who have registered through a SIP server, and where they are located. When a user agent registers with a Registrar server, a REGISTER request is made.(Rosenberg et al., 2002).

Address-of-Record (AoR): is a database that holds SIP User Id and contact information binding. To be used for AoR resolution.

Wireless Ad hoc Networks are collections of autonomous nodes forming a temporary network without the aid of any centralized administration. One of the challenges facing MANETs is Quality of Service (QoS) control for multimedia applications (Corson & Macker, 1999). This is the core of our core work in this paper

2.2. Related Work

This section briefly highlights the most relevant and recent papers found in literature that relates to modeling a voice service over MANETs using SIP as baseline protocol to fulfill the aim.

In 2010, Aburumman et al. proposed in a master thesis a solution to that uses service discovery component as interface to discover the voice service using a secure SIP functionality in Ad hoc networks by combining Distributed SIP Location Service (DSLS) with two security techniques used; the Digest Authentication Access (DAA) and Simple/ Multipurpose Internet Mail Extensions(S/MIME). DAA, S/MIME are used to secure log in service for users and data exchanged between proxies; respectively. (Aburumman, Almomani, & Akhras, 2010)

In 2011, Kagoshima et al. MANET proposed an emulator architecture and local multipath routing suitable for SIP services. MANET emulator implementation confirmed the correct operation of a SIP service from the rise of a request for session establishment, the establishment of voice packets, to the end of the session. They also tested that the local multipath routing provides a high probability of retaining the required path using an enhanced adaptive AODV routing protocol adaptive considering SIP service (Kagoshima, Kasamatsu, & Takami, 2011).

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). Todoroki et al. proposed and implemented architecture for MANET emulator for SIP services deployment called SIP_MANET emulator. This architecture supports real-time communication, node mobility, and P2P communication (Todoroki, Kagoshima, Kasamatsu, & Takami, 2012).

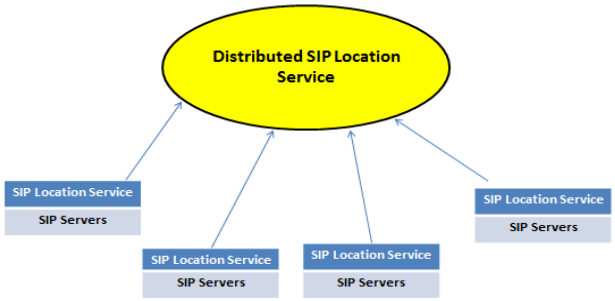

Figure 2. Distributed SIP Location Service

As noticed in literature the implementation of voice service over MANETs did not cover all the implementation factors to make a success model of such implementation, lacking either scalability or security factors; these factors are very important for implementing SIP over MANETs, if service meant to survive. Our proposed model in this paper is an extension of our previous thesis work and link to our future's Implementation. The proposed model relies on nomination-based model using trust level ranking to make the service scale better and survive longer as will be explained in the next section.

3. SYSTEM MODEL AND DESIGN

This section discusses the proposed mechanism by analyzing each part of the proposed mechanism and its suitability to be implemented for MANETs. Finally, we perform a simulation of the proposed mechanism.

Due to the decentralized nature of MANETs, we replace SIP location service at the SIP Proxy Server (PS) with a distributed SIP location service as shown in figure 2.

How it Works (Figure 3):

I. System Start-up

The proposed mechanism uses SIP PSs to act as the Registrars to maintain the address-of-record (generally a device-independent long-term identity of a user, such as an email address) and it uses (1) S/MIME multipart/signed Data (i.e. that specifies how to support authentication and integrity services via digital signature)

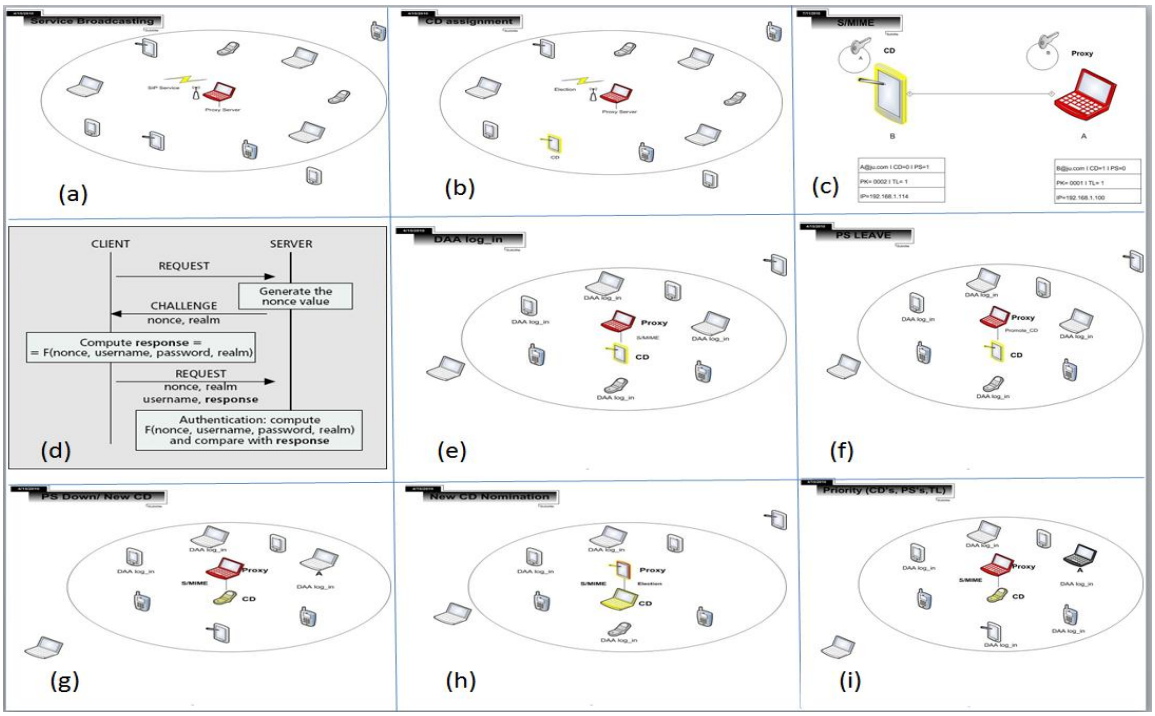

Figure 3. Nomination-Based SIP service for MANET

(a) Service Announcement. (b) CD assignment. (c) S/MIME. (d) DAA. (e) Nodes Log-in. (f) PS LEAVE. (g) PS down/New CD. (h) New CD Nomination (i) Priority (PSs, CDs, TL)

for the PSs and (2) uses pre-shared keys to log into the service through Digest Authentication Access (DAA) to map the verified users. The process is as follows:

- On bootstrapping the network, the first node in the network will announce itself as the PS as well as announcing the service (Broadcasting) to all other nodes in its transmission range.
- The PS on the initiation will send an Election message to all nodes within its transmission range to assign a Charge D'affairs (CD) before registering any node.
- CD should be a node with capabilities (Power, Resources, and stability) to replace the PS in case of any violations of the factors considered in the selection of the CD such as Trust Level (TL) based on the number of PSs and CDs overtaken by the node. The TL of a node is initialized to 1, and then it is calculated the following function (**TL=2W (PS) + W (CD))** which gives higher priority to nodes assigned as PS over CDs; Where: **TL**: Trust level (set as one for all nodes), **W**= the weight measured by number of the times PS, and CD takeover the network.

Once the proxy finds a CD using the S/MIME, it keeps a record for the verified URI of the newly assigned CD. Once the CD is registered and authenticated, the PS adds its key to the keyring that maps to its address-of record, and the CD is officially assigned and can overtake when the functioning PS is either down or on leave as shown in Fig 3.

The S/MIME bodies are signed with the private key of the sender (who may include their public key with the message as appropriate), and the bodies are also encrypted with the public key of the intended recipient. Keying map between addresses of record and corresponding certificates to maintain authorization, authentication and integrity.

II. Nodes Registration

For nodes to register users through a non-INVITE message, they need to obtain their SIP uniform resource identifier (URI) that typically contains a username and a host name, and password. Once credentials are obtained, nodes can register themselves to the PS, and authentication will be done through DAA. Once users are verified and logged into the system, nodes can then contact any registered node through the PS. When the node gets the address of the verified node, it can perform P2P communication. If any registered node logged-out, it will have to log-in through DAA. Nodes that cannot communicate in P2P mode can contact the PS, when the destination address is no more reachable.

III. PS Leave/Down Procedure:

If the PS is about to leave for any reason (Power, mobility, etc.):

- It promotes the CD to become a PS.
- The new PS sends an Election message to all registered and logged in nodes within the LS to assign a new CD before adding any new record using the S/MIME again based on the aforementioned capabilities and criteria to be able to replace the current CD.
- Registered and logged in nodes will not feel this handover.

Some nodes may experience some slight delays for the response of their messages.

If the CD does not get any update of the address-of- record on the LS for a period of time t:

- It sends a HELLO_LIVE message to the PS. If the PS does not acknowledge, then the CD overtakes and immediately sends an Election message to assign a new CD.
- Once assigned, the CD will act as the new PS.

Nodes whose records were not updated by the previous PS will have to re-register with the new PS.

IV. CD Leave/Down Procedure:

If the CD is to leave for any reason:

- It sends a LEAVE message to the PS.
- The PS then sends an Election message to all registered and logged in nodes within the LS to assign new CD before adding any new record using the S/MIME authentication process again based on the aforementioned capabilities and criteria to be able to replace the old CD.
- If the PS gets a status notification from the CD that does not satisfy the conditions (low power, unstable, etc.) or the CD is no more responding (no ACK), the
- PS pauses its functions and sends an Election message to all registered nodes to assign a new CD.
- Once assigned, the PS resumes its functions and starts registering new nodes.

V. Important Considerations

The keyring with Public Keys (PKs) for different nodes can be used to upgrade the specific key with different trust levels (TLs) based on criteria such as Stability, Number of CD Overtakes, and familiarity. When the Election occurs, priority can be obtained using the abovementioned function and capabilities.

To ensure the success of the selection of the CD, the priority processing is as follows:

Phase1: S/MIME based selection, the key from the keyring with a higher TL is calculated by the function (**TL=2W (PS) + W (CD))** using the number of PSs and CDs overtakes. Higher weights are given to PSs due to its higher functionality in the network.

Phase2: the nominated nodes will be measured from the pre-determined criteria (e.g. Power, Stability and Distance). Feedback notification about the status of CD must be sent periodically, in order to be able to assign new Ps in case of criteria shortage.

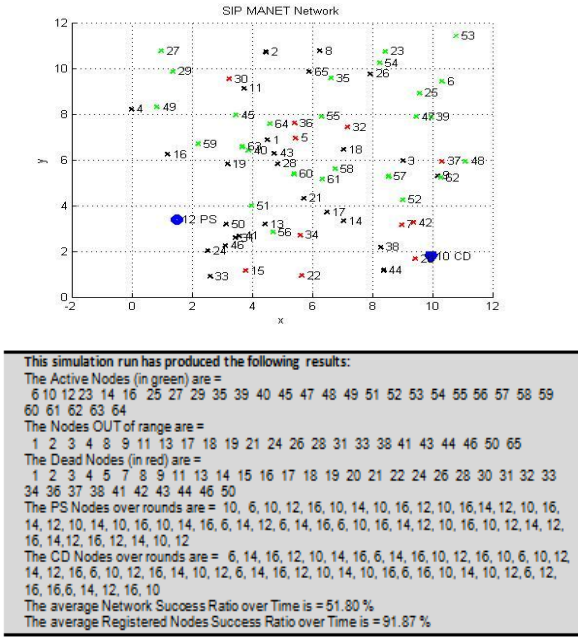

Figure 4. Simulation's Final Phase

LS updates of records must be done using highly defined conditions as follow:

-Periodic: Either (1) To send the address-of-record in the LS, every t time based on a dynamic feedback from the average work flow of the Records inserted to LS per t; Or (2) can be constant t which might add an extra overhead (messages with nothing to carry).

-Triggered: A well-defined conditions to send records when pre-determined conditions are met (e.g. Network Core or SIP-Service flow), but this would add more complexity to measure these added functions.

4. EXPERIMENTS AND RESULTS ANALYSIS

In our study we used MATLAB® to evaluate the proposed mechanism in a visual and flexible way based on the following evaluation metrics and parameter values.

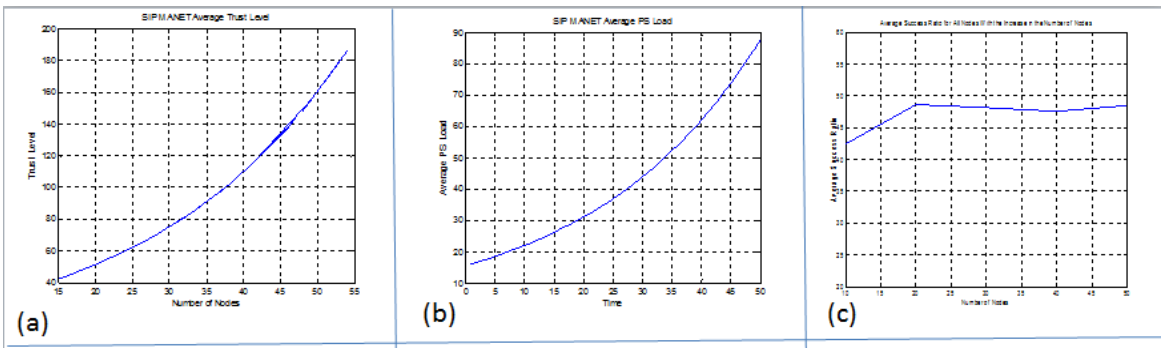

Figure 5. (a) Trust Level vs. Number of Nodes. (b) Average PS load vs. Time. (c) Average Success Ratio vs. Number of nodes.

The proposed mechanism was simulated and Figure 4 shows the simulation's final phase to be evaluated based on the following evaluation metrics:
TL: The trust level obtained by PS and CD during the S/MIME authentication process.
PS Load: Number of messages received by the Proxy Server.
Success Ratio: measures the number of success invitations to the intended recipient over time.
Scalability: The behavior of the proposed mechanism when increasing in the number of nodes.
Stability: Shows the consistency with increasing number of nodes and its effect on the service request time.
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 power of the nodes is decreased by one unit to take into consideration that the simulation time is not equivalent to one second in real networks. **Number of Nodes**: Number of nodes in the simulation environment.
Power: The measurement of power consumed in each node with the time.
Mobility: The movement of the node per time and its effect on the node.
We conducted 100 simulations, and computed the average of the findings from these 100 simulations (also taking into consideration that all the nodes are changing position (mobility) with the time).

Figure 5(a) depicts the effect of the increasing in the number of nodes on the TL. The TL was computed using our proposed equation 1. It is apparent that the TL increases as the number of nodes increases and this increase is gradual. At some stage when a PS or CD handover occurs, the average TL increases.

Figure 5(b) shows that with the increase in the network life time, the number of sent packets increases, and consequently the PS load increases. Similarly, with the increase in the number of nodes the PS load also increases.

Figure 5(c) studies the scalability 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 scalable with the increase in the network size.

5. CONCLUSIONS AND FUTURE WORK

This paper presented a mechanism to provide scalable, stable and secure SIP services for MANETS, by adapting SIP service for Ad hoc networks using a nomination-based mechanism in cooperation with the distributed SIP Location service to manage the participated nodes of SIP service. The SIP service adaptation is integrated with two security mechanisms to assure the authentication and integrity of the communicating parties at both the server and client ends. The proposed mechanism maintained the scalability and security factors for voice-service over MANETs. However, the nomination-based mechanism adds a gradual overhead as more number of nodes joins the service which is something we have an in-progress and future plans for.

Future work includes examining ways of having a more scalable system (e.g. implementing an extended cluster-based approach of SIP-Service deployment over MANETs). This could be achieved by expanding the Trust Level to reach more proxies, which would work together to form a bigger network and divide the load.

REFERENCES

Aburumman,A., I.Almomani A.Mousa(2010). Securing Session Initiation Protocol Over Ad Hoc Network. Master Thesis. University of Jordan, Amman, Jordan

Alshingiti, M. (2012). Security Enhancement for SIP in Ad Hoc Networks.Ph.D. Thesis, Carleton University.

Corson, S., and J., Macker (1999). Mobile Ad hoc Networking (MANET):Routing Protocol Performance Issues and Evaluation Considerations. *IETF RFC: 2501*.

EI Sawda, S., and P. Urien (2006). SIP Security Attacks and Solutions: A state-of-the-art review. Paper presented at the Information and Communication Technologies, 2006, ICTTA '06. 2nd, Damascus, April 24-28.

Kagoshima, T., D.Kasamatsu, and T. Kazumasa (2011). Architecture and emulator in ad hoc network for providing P2P type SIP_VoIP services. Paper presented at the TENCON 2011 - 2011 IEEE Region 10 Conference, Bali, November 21-24.

Keromytis, A.D. (2011). A Comprehensive Survey of Voice over IP Security Research. *IEEE Communications Surveys & Tutorials*, *14*(2), 514-537.

Kumar, A. (2006). An overview of voice over internet protocol (voip). *Rivier College Online Academic Journal*, 2(1), 1-13.

Rosenberg, J., H.Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, E.Schooler (2002). SIP: session initiation protocol: RFC 3261, Internet Engineering Task Force(IETF).

Sparks, R. (2007). SIP: basics and beyond. *Queue*, *5*(2), 22-33.

Todoroki, H.,T. Kagoshima, D. Kasamatsu, and K. Takami (2012). Implementation of a peer-to-peer-type SIP client application on a MANET emulator. Paper presented at the TENCON 2012 - 2012 IEEE Region 10 Conference, Cebu, November 19-22.