A Domain-Based Multi-cluster SIP Solution for Mobile Ad Hoc Network

Ala' Aburumman(✉) and Kim-Kwang Raymond Choo

Information Assurance Research Group, School of Information Technology and Mathematical Sciences, University of South Australia, South Australia, Australia
ala_fahed.aburumman@mymail.unisa.edu.au,
raymond.choo@unisa.edu.au

Abstract. Mobile Ad Hoc Networks (MANETs) are an active and challenging area in computer network research. One emerging research trend is the attempts in implementing or adapting existing voice protocols over MANETs. Successful implementation of voice over MANETs would allow an autonomous way to communicate. Session Initiation Protocol (SIP) is one of the most widely-used signaling protocols used in VoIP services. In order to implement a voice protocol over MANETs, SIP is generally required to be adapted for use over the decentralized environment instead of the overlay infrastructure-based networks. This paper proposes a Domain-Based Multi-cluster SIP solution for MANET. Our proposed solution eliminates the shortcomings of centralized approaches such as single point of failure and provides a scalable and reliable implementation. In addition, it reduces the overhead in existing fully distributed approaches. We then simulate and evaluate the proposed solution under different conditions and using metrics such as Trust Level, Proxy Server (PS) Load, Network Delay, Success Rate, and Network Management Packet.

Keywords: Mobile ad hoc networks (MANETs) · Session initiation protocol · Wireless ad hoc networks · Voice over IP (VoIP) · Voip over manets · Domain-Based Multi-cluster SIP

1 Introduction

In the past decade, there have been significant advances in the wireless arena and, consequently, we have witnessed an increase in consumer adoption of wireless technologies. An example of a widely used consumer product is Voice over IP (VoIP) that delivers multimedia over Internet Protocol (IP) networks (rather than using the Public Switched Telephone Network - PSTN). The two most popular signalling protocols for an IP-based network are the H.323- defined by the ITU, and the Session Initiation Protocol (SIP) - defined by the IETF. Increasingly, SIP is becoming more popular than H.323, mainly due to SIP's flexibility and relative simplicity [1]. Due to the popularity of 802.11/Wi-Fi enabled devices with more powerful built-in capabilities such as smart mobile devices (e.g. iOS and Android devices), Ad hoc networks can be used to support VoIP and other applications. For example, students physically present on the same

J. Tian et al. (Eds.): SecureComm 2014, Part II, LNICST 153, pp. 267–281, 2015.
DOI: 10.1007/978-3-319-23802-9_21

campus can communicate with each other using MANET-based VoIP [2]. However, implementing VoIP services over MANETs remains a challenge due to the inherent characteristics of MANETs (e.g. self-configuration of IP addresses).

One possible solution is to modify VoIP signalling services in order to support decentralized infrastructure-less networks. However, we would need to modify existing SIP services for deployment in a peer-to-peer (P2P) communication environment without compromising on availability, flexibility and efficiency (e.g. accepted call ratio) [1, 3].

In this paper, we propose a secure domain-based multi-cluster SIP solution for mobile Ad hoc network (MANET) that achieves scalability, reliability and availability.

In our proposed solution, we build a cluster-based logical overlay network on top of the network's nodes using a mechanism to minimize the overhead on the cluster heads by splitting and merging the cluster into smaller clusters in the same domain (see Sect. 3). This is designed to allow SIP users to communicate with each other either directly or to request for contact information from the logical SIP servers distributed among the network; allowing us to solve the bottleneck issue due to a standalone SIP server serving numerous client requests. In addition, our proposed solution employs security mechanism on different levels (i.e. servers and clients). To the best of our knowledge, this is one of very few publications to date that supports the secure use of SIP over MANETs. This is, probably, due to the fact that SIP has its own architecture that is based on several servers, which is more suitable for networks with a predefined infrastructure.

This paper is organized as follows: Sect. 2 reviews the background and related work. Section 3 describes our proposed domain-based cluster-based SIP solution for MANET. Our experiment setup and findings are presented in Sect. 4. Finally, Sect. 5 concludes this paper.

2 Background and Related Work

2.1 Background

The term VoIP refers to the use of IP to transfer voice. SIP, an application layer open standard developed by the IETF, is defined in RFC3261 [4]. It is a transport-independent, text-based, request-response paradigm and flexible signalling protocol, initially designed to accommodate multimedia sessions. Fundamentally, SIP is used for initiating, managing and terminating the multimedia sessions for voice and video across packet switched networks. SIP sessions generally involve one or more participants with SIP-enabled devices [4, 5].

SIP builds an overlay network on top of regular infrastructure IP-network by using the set of (following) entities communicated via SIP messages.

- User Agent (UA) is a SIP endpoint that interacts with the user.
- Servers (Proxy, Registrar and Redirect) communicate with each other or with the UA providing service.
- Gateway translates SIP into other protocols. Usually, gateways are used to connect SIP networks to the PSTN [4, 5].

An overview of a typical SIP overlay network architecture is illustrated in Fig. 1.

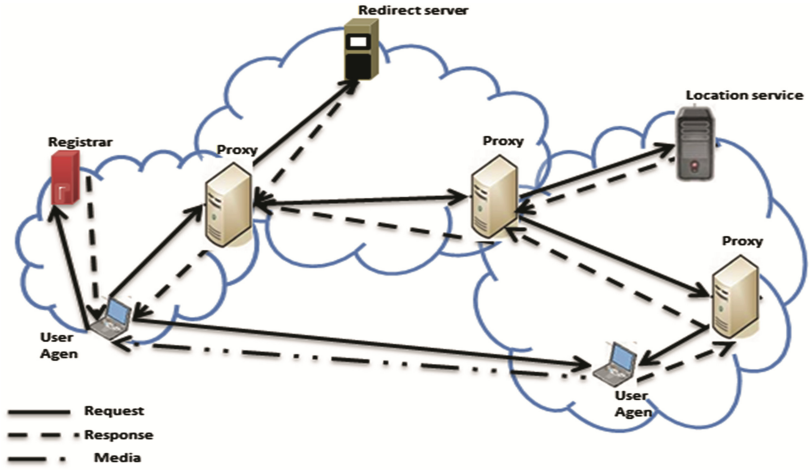

Fig. 1. SIP overly network architecture.

An Address of Record (AoR) is a SIP User Resource Identifier (URI), which is the SIP's addressing schema to call SIP users. AoR points to a domain with a location service that maps the URI to another where the user might be available [4].

It is important to differentiate between securing SIP-enabled sessions and SIP security. The former is ensuring the security of media data exchanged between parties. The latter is concerned with the exchanged SIP signaling. Like other protocols on the IP stack, SIP may suffer from various vulnerabilities. Despite the diverse security mechanisms that have been proposed for SIP-based applications [4, 6], securing SIP-based applications remain an active research challenge.

Wireless ad hoc networks are collections of autonomous nodes forming a temporary network without any centralized administration. They differ from traditional wired networks in several characteristics. For example, wireless nodes must track changes in the network in the absence of an administrator point in the network [2, 3]. Thus, establishing a secure VOIP session in such a distributed environment is a challenging task. Since SIP is the dominating signaling protocol for VoIP service, it is more practical to deploy secure SIP (rather than another signaling protocol) in a real-world implementation.

2.2 Related Work

Rebahi et al. [7] proposed the integration of a fully distributed certification authority (FDCA) as the underlying protocol for the public key infrastructure mechanism. FDCA makes use of a threshold scheme to maintain a secure SIP for Ad hoc networks' entities. It assumes the existence of a Certification Authority (CA), which issues certificates and maintains the certificate database. However, Rehabi et al.'s proposed security mechanism adds a significant overhead and the scalability factor was not considered in the implementation.

Leggio et al. [8] proposed a solution that inserts a set of the basic functionalities of a SIP proxy and registrar server in every mobile node forming a MANET. In this mechanism, the Registrar functions as an access port to manage the SIP location service entity, whereas Proxy Servers logically access the location service. User terminals can use their SIP clients in MANETs as well as in infrastructure networks. Although this proposed solution has a logical distribution of voice service over MANET, scalability and security were not thoroughly considered.

Bai et al. [9] presented a test-bed infrastructure for distributed wireless VoIP SIP servers. The architecture consists of centralized servers, and a SIP server and an Authentication, Authorization, and Accounting (AAA) server. However, the proposal used a centralized approach based on distributed servers, which may not be suitable for deployment in a decentralized environment (e.g. Ad hoc networks).

Bah [10] proposed a business model for service provision in standalone MANETs, which defines the business roles and the relationship, and interfaces between them. Bah also proposed (1) a service invocation and execution architecture to implement the business model based on the overlay network, and (2) a distribution scheme of the SIP servlets engine. The overlay network enables self-organization and self-recovery to take into account MANET's characteristics. The proposed solution is designed for a business model in a closed environment setting, which is much easier to deal with as long as the distribution of the voice service and security mechanisms is pre-agreed. It may not, however, be a viable option for everyday use in an open environment.

Kagoshima et al. [11] proposed an emulator architecture and local multipath routing suitable for SIP services. Their MANET emulator implementation demonstrated the feasibility of operating a SIP service from the time a request for session establishment is received to the establishment of voice packets and to the end of the session. The implementation also suggested 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. However, this is only a simple test bed with limited nodes to implement voice and video services in Ad hoc networks. In addition, their work did not consider various important factors such as performance analysis, scalability and security.

Alshingiti [12] proposed an enhanced security mechanism for SIP over Ad hoc networks, by introducing an extension to the SIP header. This is done by combining Cryptographically Generated Addresses with the social network paradigm to provide authentication and message integrity. The proposed mechanism includes a reasonably secure mechanism to distribute an adaptive voice service for MANETs, but it adds a significant overhead and, again, the scalability factor was not considered.

Leggio et al. [13] proposed an architecture for MANET emulator in SIP service deployment (SIP_MANET emulator), which uses AODV protocol as the underlying routing protocol. A simulation of a test implementation to deliver voice and video services in Ad hoc networks was conducted using a small number of nodes. However, the study did not consider factors such as performance analysis, scalability and security.

In our previous work [14], we presented a secure nomination–based solution to implement SIP functionality in Ad hoc networks by combining Distributed SIP Location Service with two security techniques, namely; the Digest Authentication Access (DAA)

and Simple/Multipurpose Internet Mail Extensions(S/MIME). Both DAA and S/MIME are used to provide secure log in service for users and data exchanged between proxies respectively. In the proposed solution, a node is elected to be a proxy server (PS) that handles SIP functionality and another node, Change D'affair (CD), is elected to be a backup for the server. The proxy is set to be the first node in the network, and then it will broadcast an election message to select a CD to be the next proxy after the PS delivers the task to the elected CD.

Abdullah et al. [15] proposed a secure cluster-based SIP service over Ad hoc network to protect the adapted SIP service from several types of attacks. This research eliminates the shortcomings of centralized approaches such as single point of failure, as well as reducing the overhead presented in fully distributed approaches.

It is clear from the literature that improving the scalability and security of SIP services on MANETs is an ongoing research challenge. This is not surprising as SIP relies on the resources of server functions, and unfortunately in a MANET environment, servers have limited resources. As the size of the network increases, the load on the servers increases, and consequently, this decreases their reliability and availability. In addition, the dynamic, unpredictable and self-configuring nature of MANETs complicates efforts to maximize the scalability and security of SIP services over MANETs.

The aim and novelty of this paper is the proposed solution to overcome the scalability shortcoming of MANETs in a secure manner. This is done by implementing a mechanism on the organizational level of the application layer using a domain-based dynamic clustering with a built-in reputation function to maintain the best selection of the servers based on a feedback from the network core and key ranking equation to implement an adaptive SIP solution over MANETs.

3 Our Proposed Solution

This section describes our proposed Domain-Based Multi-cluster SIP solution for MANET, which allows calls to be established between peer-nodes ubiquitously using infrastructure-less environment. It is assumed that the SIP application can perform at least one-hop message broadcasting (Fig. 2).

In the proposed solution, SIP entities comprise SIP User Agent (UA) and SIP Proxy (a combination of SIP Registrar and SIP Discovery Server - SIP DS), and are implemented on the protocol stack. Nodes can also function as Registrar or as DS to register other SIP UAs or provide address-of-record (AoR) resolution respectively.

We note that a number of researchers have demonstrated that cluster-based solutions can address various limitations associated with Ad hoc networks such as in routing, traffic coordination and fault-tolerance [5]. Therefore, our proposed solution builds logical clusters over the SIP network at the application level. The formation of SIP network's clusters is based on nodes' positions within the network and the neighborhood degree. This approach eliminates the need for additional message types as it reuses the well-known SIP messages by adding special headers. The latter is used to indicate the nature of the exchanged message. The clusters consist of Cluster Head (CH) nodes which act as SIP DS. The terms CH and SIP DS (or SIP server) are used interchangeably in this paper.

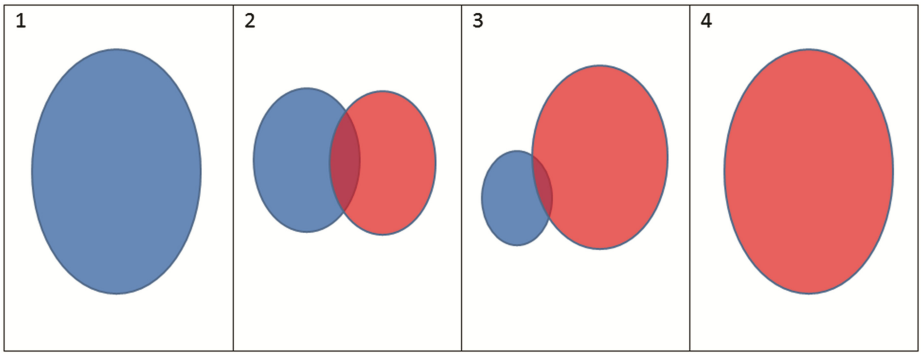

Fig. 2. Logical diagram – cluster splitting and merging. (1) Cluster reaches saturation limit. (2) Cluster splits into two separate clusters. (3) A cluster reaches minimal count. (4) Merges with an appropriate cluster.

Naturally, we assume that the network is vulnerable to attacks. For example, external attackers can launch various attacks targeting the availability of the SIP network (e.g. poisoning information to SIP users so that the SIP network is unable to establish calls). We also assume that SIP users will pre-share or establish their security associations with each other (e.g. they have exchanged their security keys offline or via other secure means). All SIP users are capable of using basic security algorithms such as Message Authentication Code algorithm.

The aim of our solution is to support both standard and ad-hoc SIP operations with the following design goals:

- Enabling Ad hoc node peers to establish calls over the decentralized environment of Ad hoc network based on SIP;
- Overcoming existing limitations of relying on static, fixed, and centralized entities;
- Preventing unnecessary expensive overheads (e.g. eliminating the need to distribute all SIP functionalities over the entire network) without affecting scalability or resulting in higher energy and bandwidth consumption; and
- Compatibility with the standard SIP.

Next, we will outline the modifications required to the standard components in MANETs to implement our proposed solution.

3.1 MANET Clustering

For MANET networks to utilize SIP for VoIP, we need SIP servers for the initialization and teardown of the P2P sessions as well as AoR resolution. Since MANET is a flexible network without any supporting infrastructure, the selected server needs to be one of the nodes within the MANET. These nodes typically have relatively little CPU power and battery life, and consequently, limiting the number of users in this service before latency issue occurs. To address this limitation, we use a clustering mechanism to dynamically elect or retire servers to load balance based on demand (see Sect. 3.4), which ensures a uniform service level.

3.2 Proposed Server Functionality

Primary Server (PS) is a node elected to act as a SIP Proxy and Registrar server to transmit and receive P2P connection requests for the nodes in the cluster that it manages.

This server maintains three different tables containing node data (Local Node, Global Node and Server). The PS has other duties, namely: servicing special invite requests of new nodes and merging and splitting the cluster based on the node count.

The Backup Server (BS) is a backup node that will take over or be promoted to act as the PS if the PS goes offline as well as supporting the PS with load balancing functionality. The BS keeps an identical set of the tables containing node data.

3.3 Reputation-Based Election

Using a reputation-based technique to select a PS or BS ensures that the chosen server is a trusted entity [12]. However, in such an approach, the preference of a server needs to be updated each time they are elected, affecting the stable operation of the network. To avoid this limitation, we propose a priority algorithm (see Eq. (1)) that takes into account the amount of time that a server has been operational when increasing its priority. This is to ensure that reliable servers are selected in preference to others.

Our proposed priority algorithm is as follows:

$$\text{Priority} = \text{RPC} + ((\text{SU2})/10) \tag{1}$$

In the algorithm, RPC denotes the Reputation Point Count and SU denotes the Server Uptime. The initialization value of RPC for both the Backup server and the primary server needs to be different. For example, in our experiment, RPC is initialized to 1 when computing the priority value of the Backup server and RPC is initialized to 3 for the primary server, and an SU of 10 units will result in a priority value of 11 for the Backup server or 13 for the primary server.

The priority algorithm computes the reputation of selected functioning servers, which is used to determine their eligibility to serve as the PS or BS. To achieve a higher priority score, potential servers will have to either serve longer in the network (SU) or maintain higher roles (PS, BS). Our priority algorithm gives preference to a longer serving server than one who has served for a shorter period in different roles.

3.4 Proposed New Clustering Mechanism

The proposed clustering mechanism assigns one server to a specified set of nodes referred to as a cluster head. Each cluster has a maximum and a minimum saturation limit of nodes, which is used to trigger the respective cluster split and merge sequences. In a cluster split sequence, the BS node becomes the PS in the new cluster taking half of the nodes and then performing an election to select a BS. Once a cluster falls below the minimum saturation limit, the PS of that cluster will send merge requests to other clusters to amalgamate into an efficient cluster size.

3.5 Server's AoR Entities

The Local Node Table holds records of the local in-cluster nodes installed on every server and contains the Name, Status, Priority and Offline duration for all nodes in the cluster. This table is stored on both on PS and BS to keep track of all nodes in the cluster. The Global Node Table contains a list of all registered nodes in the domain, and each node can only be updated by their respective PS or BS. The table is distributed and installed on all in-domain active servers (participating clusters).

The Server Table contains information about the cluster servers such as Type, Public keys, Cluster ID, Server name and Priority. The priority field of the server cannot, however, be updated by itself – this field can only be updated by the in-domain active servers (cluster heads).

4 Experiment Setup and Findings

4.1 How Does the Proposed Solution Work?

Startup: The first node to initiate the service with a domain-name is the PS acting as a CH. In addition to the role of PS, the CH functions as the Registrar to maintain the AoR (generally a device-independent long-term identity of a user, such as an email address). The process is outlined in Fig. 3.

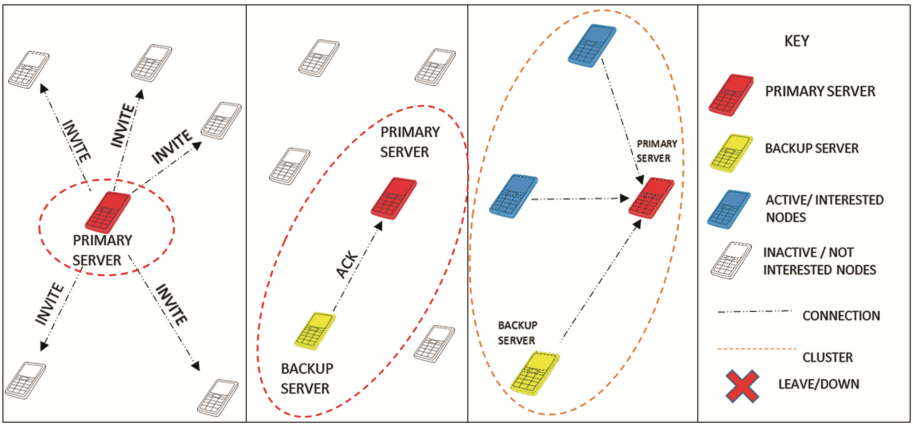

Fig. 3. Startup

On startup, the node initiating the service will advertise to all other nodes that are in range of the service. The first interested and eligible node to act as the BS will respond with an ACK command, which will be authenticated (e.g. using S/MIME security mechanism [12]). Once this node has been accepted as the BS, all subsequent nodes that send ACK's will be added as regular nodes to the service.

Primary Server Leave/Down Procedure: Should the PS exit the service (e.g. due to insufficient battery power), the BS will be promoted to be the new PS by the departing PS. The new PS sends an Election message to all registered and currently logged in nodes in the cluster to select a new BS and this must be done before any new node can be registered with this cluster.

The new BS is selected based on its priority. If no trusted node can be found to be elected to act as a BS, then a node will be selected by the new PS to act as the BS.

The handover process should not affect any client node cluster affiliation or the progress of already initialized SIP P2P communications, although there might be minor delays for nodes in the process of sending messages to the server. If the server goes offline unexpectedly or the BS does not hear from the PS for a pre-determined duration, then the BS is automatically promoted to be the PS temporarily until a server election is performed to select new servers (see Fig. 4).

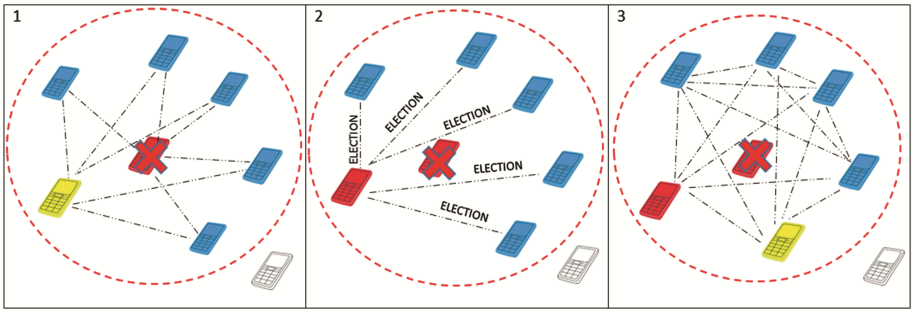

Fig. 4. Primary server leave/down procedure

Backup Server Leave/Down Procedure: If the BS exits the service:

- The BS will send a LEAVE message to the PS, and
- The PS will send an Election message to all registered and currently logged in nodes in the cluster to select a new BS and this must be done before any new node can be registered with this cluster

The new BS is selected using the procedure described in the previous Section. If no trusted node can be found to be elected to act as a BS, then a handshake is performed with an adjacent node to the PS and this node is now the BS.

The handover process should not affect any client node cluster affiliation or the progress of already initialized SIP P2P communications, although nodes sending messages to the server may experience minor delays. If the server goes offline unexpectedly and the PS does not hear from the BS for a pre-determined duration, then the PS triggers another server election to select a new BS.

Clustering Function: If the cluster reaches its saturation limit of nodes, the PS splits the table giving half the nodes to the BS, and the BS adds these nodes to a new Local Node table. BS will then create a new cluster and notify all his/her nodes with a new Cluster ID and Server ID. Both servers will also notify the other servers in the domain

of the updates to their global node and server tables. An election is done in both clusters to ensure the best selection of servers.

Merging Function: When the Cluster reaches a minimum count threshold, the PS will find another cluster to join. Note that PS1 and PS2 denote the Local Primary Server and the Remote Primary Server respectively.

1. PS1 sends a GETCOUNT message to all other PS in the domain, which will respond with their node count;
2. PS1 selects the cluster with the smallest count of nodes;
3. PS1 sends a MERGE command to the selected cluster's PS (PS2);
4. If an ACK message is received from PS2, PS1 will notify his/her nodes providing PS2's Cluster ID and Server ID. Otherwise, PS1 will send a merge request to the next smallest cluster This process will repeat until PS1 successfully join a cluster;
5. PS1 sends its local node table to PS2;
6. PS2 adds the local node table values to its table and cluster;
7. PS2 notifies all other servers in the domain of the updates to their global node and server tables;
8. PS1 dissolves to a regular node; and
9. PS2 calls election in the merged cluster (see Fig. 5).

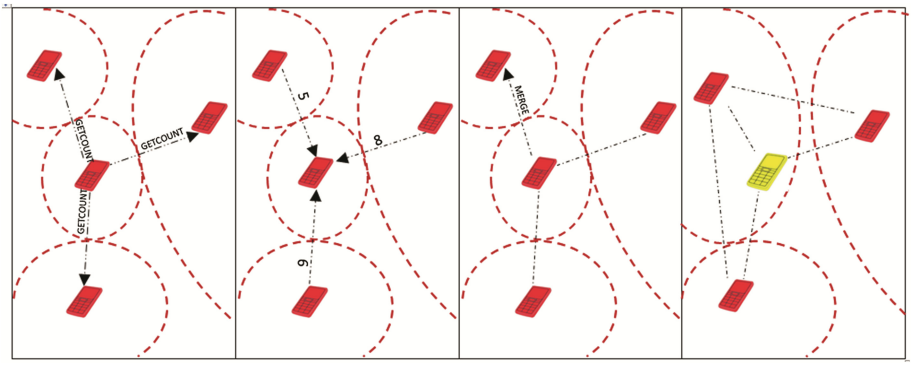

Fig. 5. Cluster heads merge/join procedure

When a node goes offline, the PS will remove their entry from the local node table prior to notifying other servers in the domain. The entry will only exist in the global node table for the period of 24 h (or a pre-determined duration). The node will then need to apply again as a new node when rejoining the network. For security reasons, only the PS and BS are able to update the state of a node and this is cross-checked against the Server table.

Server authentication is an important consideration to ensure the security and integrity of the services. For example, a strong server authentication will prevent low priority nodes masquerading as high priority ones to rig their own election. The use of a CHAP handshake when a server is being elected could be an effective authentication method,

as the selected server would come into direct contact with the server that is electing it. This would prevent man in the middle attacks. Real-time blocking of accounts which was found to be in violation of policies (e.g. multiple logins from different locations and on different devices) is another effective way to mitigate risks associated with compromised accounts in a timely manner.

4.2 Findings

Our simulation of the proposed solution is described in this section, and we evaluate using the following evaluation metrics and parameters:

- PS Load: The number of messages received by the PS.
- Success Rate: The number of invitations successfully delivered to the intended recipient over time.
- Scalability: The behavior of the proposed mechanism when the number of nodes is increased.
- Stability: Shows the consistency with increasing number of nodes and its effect on the service request time.
- Time: The amount of time in seconds for the running of the network. For each second of 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-time network.
- Power: The measurement of power consumed in each node.
- Mobility: The movement of the node and its effect on the node.

We conducted 100 simulations under different conditions, and computed the average of the findings (also taking into consideration that all the nodes are changing position (mobility) with time).

Figure 6 presents the findings of the effect of PS load over the lifetime of the network. When the cluster was first established, the number of nodes within the cluster will increase (due to new registration) and eventually reach a point of stability. Once the threshold values are reached, the clustering process (i.e. merge or split) will commence. For example, as shown between the values of 115–134 on the X-axis of Fig. 6, the Merge process is triggered, and between the values of 248–267 on the X-axis, the Split process is triggered resulting into the forming of another cluster.

As shown in Fig. 7, the success rate is consistent and does not degrade over time. This is due to the network load being divided by the dynamic multi-clustering mechanism, resulting in a fair distribution of the load carried by each cluster. It is recommended that the threshold values (that trigger the Merge and Split process) be determined only after an in-depth analysis of the network behaviour to provide an optimal performance.

As shown in Fig. 8, our multi-clustering approach has significantly increased the number of participating nodes; addressing one of the challenging issues of MANETs (i.e. the overall management of the voice service was divided into clusters to evenly share the network load on dynamic clusters in the same domain). It is also worth pointing out that the cluster may fail to register nodes in the merge process occasionally, which may cause a visible drop in the number of nodes such as the example between the values

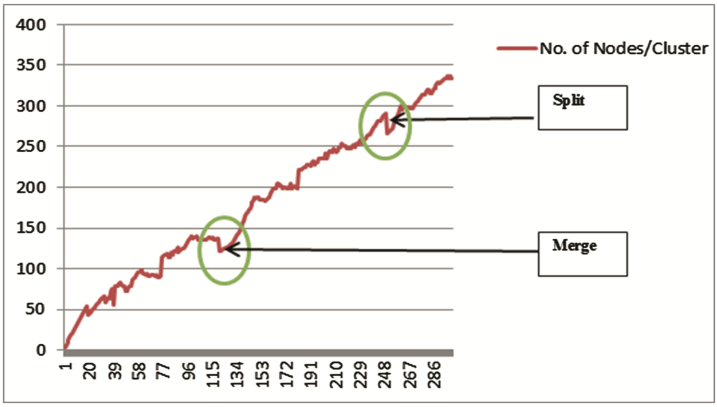

Fig. 6. Number of nodes per cluster over time

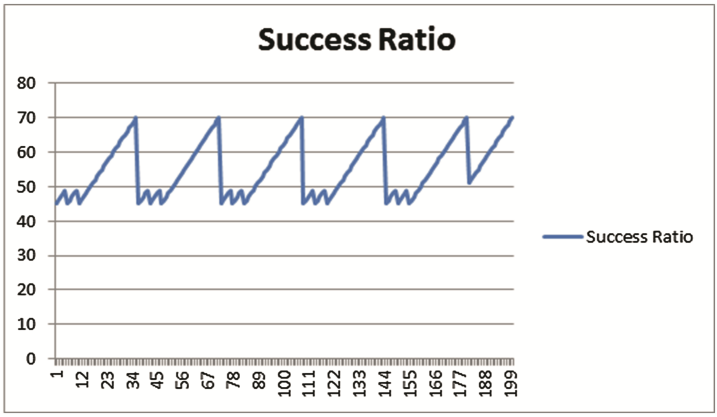

Fig. 7. Stability (success rate)

of 37–49 on the X-axis of Fig. 8. Those nodes can, however, re-register directly under any other cluster in the same domain and will be connected and added to the global table record. The noticeable sudden increase in the number of nodes between the values of 133–145 on the X-axis is due to the increase in the number of nodes interested in joining the network (e.g. peak/rush hour), which results in multiple splits of the clusters to register more nodes.

Figure 9 shows the reputation (server uptime) which ensures nonlinear growth of priority over time for this disparity between time, and points rewarded ensures the most stable servers are preferred (i.e. based on number of times the cluster heads and backup server were selected).

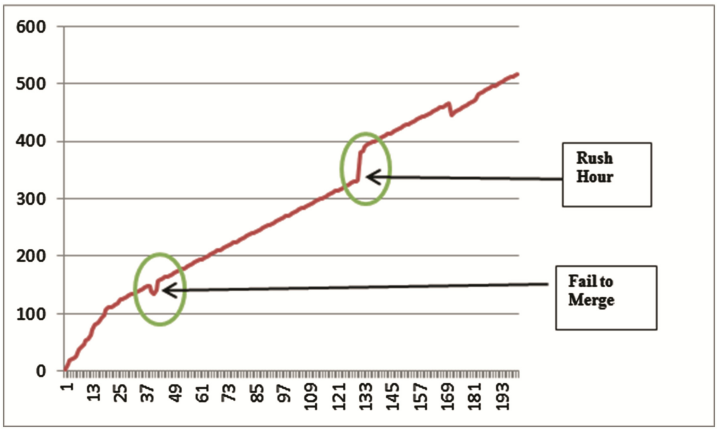

Fig. 8. Scalability (number of nodes against the simulation time)

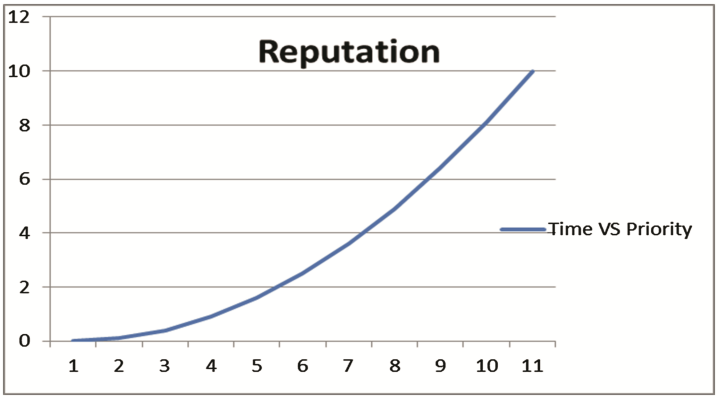

Fig. 9. Reputation (server uptime)

Our proposed mechanism has addressed issues previously identified in [14, 15]. As shown in Table 1, the domain-based dynamic clustering solution significantly enhanced the scalability factor of MANETs by adapting a SIP solution on the application layer to virtually organize and administrate the network in a dynamic way based on pre-determined thresholds to trigger the point of optimal performance. The security of the solution is also enhanced by the integration of our proposed priority algorithm as a way of quantifying the trust level. While the number of nodes in our previous mechanisms [14] was limited to a maximum of 50 nodes, this proposed solution can accommodate up to 350 nodes. In addition, our proposed solution has reduced the average number of management packets and provides a more flexible way to divide the overhead over the network, which stabilized the network and maintained an optimal performance.

Table 1. Comparative summary

	Nomination-based [17]	Cluster-based [18]	Domain-based multi-cluster
Priority	Static	Static	Dynamic
Scalability	Up to 50 nodes	Up to 80 nodes	Up to 350 nodes
Av. No. management packets	Stable	Gradual increase	Gradual increase
Stability	Limited	Limited	Flexible
Overhead	High	Varies	Average

5 Conclusion and Future Work

In this paper, we proposed a Domain-Based Multi-cluster SIP Solution for MANET that results in a stable, secure and scalable MANET service. Our proposed solution includes an advanced clustering technique designed to overcome the shortcomings of the adapted nomination-based mechanism in our previous work [14]. We simulated our solution under different settings and using different metrics and parameters. The findings demonstrated the utility of our proposed solution. Future work includes conducting user studies where we implement and evaluate our solution with student and staff mobile participants on the University campus.

References

1. Garber, M.: Securing session initiation protocol over ad hoc network. Master thesis, Institute for Pervasive Computing, Zurich (2005)
2. Basagni, S., Conti, M., Giordano, S., Stojmenovic, I.: Mobile Ad Hoc Networking. Wiley, New York (2004)
3. Stuedi, P., Bihr, M., Remund, A., Alonso, G.: SIPHoc: efficient SIP middleware for ad hoc networks. In: Cerqueira, R., Campbell, R.H. (eds.) Middleware 2007. LNCS, vol. 4834, pp. 60–79. Springer, Heidelberg (2007)
4. Rosenberg, J., et al.: SIP: session initiation protocol. RFC 3261, IETF (2002)
5. Sparks, R.: SIP basics and beyond, estacado systems. ACM Queue **5**(2), 22–33 (2007)
6. Arkko, J., Torvinen, V., Camarillo, G., Niemi, A., Haukka, T.: Security mechanism agreement for the session initiation protocol (SIP), RFC 3329. In: IETF (2003)
7. Rebahi, Y., et al.: SIP-based multimedia services provision in ad hoc networks. In: MAGNET Workshop on My Personal Adaptive Global Net: Visions and Beyond, Shanghai, China (2004)
8. Leggio, S., et al.: Session initiation protocol deployment in ad-hoc networks: a decentralized approach. In: 2nd International Workshop on Wireless Ad-hoc Networks (IWWAN 2005) (2005)

9. Bai, Y., Aminullah, S., Han, Q., Wang, D., Zhang, T., Qian, D.: A novel distributed wireless VoIP server based on SIP. In: IEEE International Conference on Multimedia and Ubiquitous Engineering (MUE 2007), pp. 958–962 (2007)
10. Bah, S.: SIP servlets-based service provisioning in MANETs. Concordia University (2010)
11. Kagoshima, T., Kasamatsu, D., Takami, K.: Architecture and emulator in ad hoc network for providing P2P type SIP_VoIP services. In: 2011 IEEE Region 10 Conference (TENCON 2011), pp. 164–168 (2011)
12. Alshingiti, M.: Security Enhancement for SIP in Ad Hoc Networks. Carleton University, Ottawa (2012)
13. Leggio, S., Miranda, H., Raatikainen, K., Rodrigues, L.: SIPCache: a distributed SIP location service for mobile ad-hoc networks. In: Third Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, pp. 1–8 (2006)
14. Aburumman, A, Choo, K.-K.R., Lee, I.: Nomination-based session initiation protocol service for mobile ad hoc networks. In: Gaertner, P., Bowden, F., Piantadosi, J., Mobbs, K. (eds) 22nd National Conference of the Australian Society for Operations Research (ASOR 2013), pp. 149–155. The Australian Society for Operations Research, Adelaide, 1–6 December 2013
15. Abdullah, L., Almomani, I., Aburumman, A.: Secure cluster-based SIP service over ad hoc networks. In: 2013 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT 2013), pp. 1–7 (2013)