A Secure Cross-Domain SIP Solution for Mobile Ad Hoc Network Using Dynamic Clustering

Ala' Aburumman[1], Wei Jye Seo[1], Rafiqul Islam[2],
Muhammad Khurram Khan[3], and Kim-Kwang Raymond Choo[1(✉)]

[1] School of Information Technology & Mathematical Sciences,
University of South Australia, Adelaide, Australia
{abuaa001,seowy002}@mymail.unisa.edu.au,
raymond.choo@fulbrightmail.org
[2] School of Computing & Mathematics, Charles Sturt University, Bathurst, Australia
mislam@csu.edu.au
[3] Center of Excellence in Information Assurance (CoEIA), King Saud University,
Riyadh, Kingdom of Saudi Arabia
mkhurram@ksu.edu.sa

Abstract. With the increasingly popularity of mobile devices (e.g. iPhones and iPads), Mobile Ad hoc Networks (MANETs) have emerged as a topical research area in recent years, and adapting and implementing voice protocols over MANETs is a popular area of inquiry. Successful implementation of voice over MANETs would present a more efficient and cheaper way of communication. In this paper, we propose a cross-domain Session Initiation Protocol (SIP), a widely used voice over Internet Protocol (VoIP) protocol, solution for MANETs using dynamic clustering by extending the scheme of Aburumman and Choo. Our enhanced solution allows us to scale across domains, and deal with outbound requests using the reputation method. Advantages of this solution include avoiding the shortcomings associated with centralized approaches, such as a single point of failure. To demonstrate the utility of the solution, we simulate and evaluate the proposed solution under different conditions and using metrics such as trust level, overhead, network delay, success ratio, and network management packet.

Keywords: Mobile Ad hoc Networks (MANETs) · Session initiation protocol · Security · Privacy · Wireless ad hoc networks · Voice over IP (VoIP) · VoIP over manets · Cross-domain · Dynamic clustering SIP · Network Simulator 3 (NS3)

1 Introduction

Wireless devices are an integral role in our daily communications, supporting applications such as Radio Frequency Identification (RFID) and Voice over Internet Protocol (VoIP). VoIP, for example, can be used to deliver voice and video contents over the internet in real-time, instead of the Public Switched Telephone Network (PSTN) [17][18]. In the past decade, there have been significant advances in the

© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2015
B. Thuraisingham et al. (Eds.): SecureComm 2015, LNICST 164, pp. 649–664, 2015.
DOI: 10.1007/978-3-319-28865-9_43

wireless arena; consequently, we have witnessed an increase in consumer adoption of wireless technologies. 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 in RFC3261 [4]. Increasingly, SIP is becoming more popular than H.323, mainly due to SIP's flexibility and relative simplicity [1][2]. 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) [19], Ad hoc networks can be used to support VoIP and other applications. For example, students physically present on the same campus can communicate with each other using MANET-based VoIP services [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 potential solution is to modify VoIP signalling services in order to support decentralized infrastructure-less networks. The challenge, however, is 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 Cross-Domain SIP solution for MANETs using dynamic clustering to provide scalability, reliability and availability. In the proposed solution, we extend the cluster-based logical overlay network from our previous work [16] by introducing new functionalities to the proposed entities with an enhanced reputation equation. The solution would 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; thus, solving 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). As found in literature, this is one of 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, which is more suitable for networks with a predefined infrastructure.

This paper is organized as follows: Section 2 reviews the background and related work. Sections 3 and 4 describe our proposed cross-domain SIP solution for MANETs, and our implementation, respectively. We discuss the findings from our implementation in Section 5. Finally, Section 6 concludes this paper.

2 Background and Related Work

2.1 Background

SIP is a signalling protocol for initiating, managing and terminating the multimedia sessions for voice and video across packet switched networks. The main components of SIP are shown in Fig. 1 and explained below.

SIP main components are:

- User Agents (UAs) are a SIP endpoint entities that interact with other SIP components and used to either generate requests and send them to servers (i.e. User Agent Client - UAC) or receive requests, process them and generate responses (i.e. User Agent Server - UAS).

- Servers (Proxy, Registrar and Redirect) they hold a predefined set of rules to handle requests and response generated by UAs and they play the role of mediator to communicate with each other or with the UA providing service to enforce those rules.
- Location Service/Server is used to store the addresses registered by the registrar.
- Gateway is used to translate SIP to other protocols, if to be used by different type of network (e.g. PSTN [4][5].

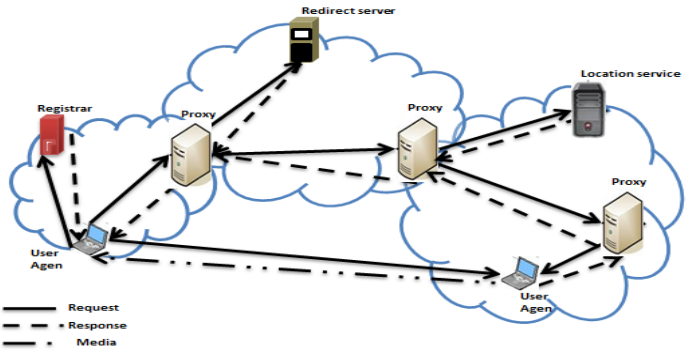

Fig. 1. SIP Overly Network architecture.

An Address of Record (AoR), a SIP User Resource Identifier (URI), allows one to call other SIP users. The AoR will point to a domain with a location service, which maps the URI to one where the user might be available.

Similar to other protocols on the IP stack, SIP may suffer from various vulnerabilities. Despite the range of security mechanisms 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. These nodes form a temporary network without the need for a centralized administration. A key difference between a wireless ad hoc network and a traditional wired networks is that in the former, changes in the network needed to be tracked due to the absence of an administrator point [2][3]. This complicates the establishment of a secure VOIP session. SIP would be more practical solution for secure SIP (rather than another signaling protocol) deployment in a real-world implementation, since it is the dominating signaling protocol for VoIP service.

2.2 Related Work

By implementing all the necessary functionalities of a SIP, Leggio et al. [7] proposed a decentralized ad-hoc network framework. This approach elects a registrar to control manage while other newcomers who joined the network are being bounded with the registrar. It is possible to have SIP services with the decentralized approach; however, the issues of fault-tolerance and scalability remain.

Bai a et al. [8] use a test-bed infrastructure to form a distributed wireless multimedia network based on SIP protocol that allow text, voice and video communication to both wired and wireless devices. Utilizing Authentication, Authorization, and Accounting (AAA) server and SIP server, Bai approach still require a centralized controlled authentication which is not application in an Ad hoc network and other decentralized environment.

Focusing on the two different MANET environments, which are standalone MANETs and Multihop Cellular Networks (MCNs), the research detailed in [9] aims to address the service provisioning aspects in both environment. The research proposed a business model that defines the relationship and interfaces of MANET and the service provision in the MANET. The approach is tailored for closed environment setting with the voice service and security mechanisms that are agreed in advance.

By using an emulator architecture and local multipath for SIP services, Kogoshima, Kasamatsu and Takami [10] built a SIP_MANET emulator, which is evaluated using a SIP_VoIP call. The simulation of SIP service in MANET suggested a high probability of preserving the required path by implementing an enhanced adaptive AODV routing protocol. The simulation was conducted in a test bed environment with limited nodes. Other important factors, such as performance analysis, scalability, and security, were not addressed in their research.

As security concerns are increasingly important in SIP services, including those for Ad hoc networks, Alshingiti [11] suggested the combination of cryptographically generated addresses (CGA) with the social network paradigm for authentication and message integrity. Although this approach did not cost traffic overhead in terms of the registration process, it significantly increases the traffic on the call establishment and termination process. Scalability of the SIP services in MANET in this approach was also not considered.

Leggio et al. [12] proposed a fully distributed location service to locating SIP users in as small scaled network to avoid a single point of failure. This is done using by embedding a sundet of SIP proxy and registrar server functionality in all nodes.

In our previous work [13], 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. [14] 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.

Almobaideen et al. [15] proposed an adapted and semi distributed SIP protocol that works using clustered MANETs (referred to as FCSIP). In FCSIP, a new role for SIP

server was introduced, where the SIP server also acts as a cluster-head to be the discovery servers to allow SIP agents to get information about other clients in the SIP cluster. It was claimed that such implementation would perform better than the fully-distributed SIP protocol over MANETs.

In [16], we presented a solution addressing the scalability limitation in a domain-based distribution of SIP services. We used a dynamic clustering to maximize the usage of resources to facilitate the deployment of SIP over MANETs. Our simulation results demonstrated that scalability of SIP service is increased, while minimizing the overheads by eliminating or dividing the workload among servers (i.e. cluster heads). However, security was not considered in this work.

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 play a limiting role. As the size of the network increases, the load on the servers increases; consequently, this affects the level of reliability and availability. The dynamic, unpredictable and self-configuring nature of MANETs also complicates efforts to maximize the scalability and security of SIP services over MANETs.

In this paper, we aim to contribute to addressing the literature gap. More specifically, we extend our previous solution in [16] in order to enhance the scalability and security of implementing SIP over MANETs.

3 Our Proposed Solution

This section describes our proposed cross-domain SIP solution for MANETs using dynamic clustering proposed in our previous work [16], 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.

In the proposed solution, we introduce the functionality of redirect servers inherited from the SIP standard protocol for Backup Servers (BS). The BS will be directing the outbound requests; requests from nodes in neighboring domains. 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.

Cluster-based solutions can address various limitations associated with Ad hoc networks, such as in routing, traffic coordination and fault-tolerance. Our proposed solution, therefore, builds logical clusters over the SIP network at the application level. In our approach, the SIP network's clusters are formed based on the positions of the nodes within the network and the neighborhood degree. Such an approach allows us to eliminate the need for additional message types, as we are able to reuse SIP messages by inserting additional headers (and indicating the nature of the exchanged message). The clusters consist of Cluster Head (CH).

We assume that the network is subject to various types of attacks. For example, external attackers could seek to flood the network with messages, which affects 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), and all SIP users are capable of using basic security algorithms, such as Message Authentication Code (MAC) cryptographic algorithm.

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

- Provide a scalable SIP service over MANET, within the constraint of the existing network;
- Enable Ad hoc node peers to establish calls over the decentralized SP-based Ad hoc network environment;
- Overcome existing limitations of relying on static, fixed, and centralized entities;
- Prevent 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
- Provide a compatible solution complying with the standard SIP.

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

3.1 Proposed Server Functionality

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

This server maintains three different tables containing node data, namely: tables for local node, global node and server. The PS has other duties, such as 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 with the capability to redirect outbound requests 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.

3.2 Proposed New Clustering Mechanism

For the SIP service to be able to be utilized by MANETs, we need SIP servers for the initialization and teardown of the P2P sessions as well as AoR resolution. Nodes in MANETs typically have relatively little CPU power and battery life; therefore,

limiting the number of users in this service before latency issue occurs. To address this limitation, we propose a clustering mechanism to dynamically elect or retire servers to load balance based on a pre-determined threshold. Once the latter is reached, a function will be automatically activated to ensure a balanced and uniform service level.

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 SPLIT and MERGE functions in the cluster forming a dynamic clustering mechanism. In a cluster SPLIT Function, the BS node becomes the PS in the new cluster taking approximately half of the nodes and then performing an election to select a BS. Conversely, MERGE function triggers 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 – see [16].

3.3 Server's AoR Entities

Address-of-records (AoR) are extended for the servers to have a global and local view of the (inbound and outbound) network, which are referred to Global Node Table (GNT) and Local Node Table (LNT), respectively. The GNT 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 (i.e. participating clusters). This is a slight variation from our work in [16], as the BS will have a field to register outbound extended-domain. Alien-domain records will be able to redirect requests to either neighboring domains (e.g. different divisions in the same university) or Alien domains (e.g. other universities). To differentiate between these two domain types, an enhanced reputation mechanism will be used to deal with such requests and decision will be made by the BS server and recorded on both PS and BS's AoR (see Section 3.4)

The LNT holds the records of the local in-cluster nodes installed on every server, which include information such as the Name, Status, Priority and Offline duration for all nodes in the cluster. This table is stored on both PS and BS to keep track of all nodes in the cluster. This arrangement also provides redundancy, in case the table in one of the servers is corrupted.

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).

3.4 Reputation-Based Election

In this section, we will use two levels of reputation-based Elections for both inbound and outbound requests. For inbound requests, a reputation-based technique is used to select a PS or BS in order to ensure 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; hence, affecting the stable operation of the network. To avoid

this limitation, we adapted our priority algorithm in [16] which 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.

For outbound requests, another reputation-based technique is used to authenticate PSs in other domains. This is done using a ranking system that uses a counter of valid digital signatures to be calculated on each PS along the way. The combination algorithm is based on extended-domain digital signatures (PS_{DS}) and Alien digital signatures (PSds) and will be recorded, updated and saved in the AOR and used on each server along the way. The final decision to authenticate this request will be made by the BS at the receiving end (i.e. the value will have to pass a minimum pre-determined threshold in order to be allowed to proceed and for the invitation to be forwarded to the intended recipient).

Our proposed priority algorithm is as follows:

$$AUTH = PS_{DS} + PS_{ds}/2 + TL_{AoR} > X \quad (1)$$

In the algorithm (see Equation 1), AUTH denotes the Reputation Point Count and TL_{AoR} denotes the Trust Level of the PSs, initialized as Zero. All servers receiving the requests will include their digital signature on outbound forwarded requests to 'earn' more points. Invalid signatures will be counted as Zero. This algorithm gives more weight to PS_{DS}, assuming that most of these domains are an extension of the same service as mentioned earlier (e.g. a division within a university). Those requests that have not passed the minimum pre-determined threshold will need to send more requests (referred to as the warm-up period).

The priority algorithm computes the reputation of selected functioning servers, which is used to determine their eligibility and authenticity as PS. To be able to scale better and achieve a higher priority score, servers will have to serve longer in the network.

Our priority algorithm sets AUTH in AoR to Zero, if PS is inactive for a significant period of time (T) using a dynamic time counter every time the record is updated. T is a dynamic decreasing timer calculated based on how active the PS involved is (Number of valid digital signatures) and the status of the outbound requests (extended or Alien).

4 Implementation

In this section, we will briefly summarize the steps involved in initiating SIP-service over MANETs in the domain level.

4.1 Service Initiation and In-domain Clustering

In the startup phase, the node initiating the service; Cluster Head and Proxy Server (CH and PS, respectively), will advertise to all other nodes that are in range of the service. The first interested and eligible node will be assigned to act as the BS.

Should the PS decides to exit the service (e.g. due to insufficient battery power or mobility), the BS will be promoted to be the new PS by the departing PS. On the other hand, if the PS or BS is to exit the service, a LEAVE message will be sent allowing to promote an eligible node to replace it.

In case of undeclared leave from both functioning servers PS or BS, either server with no backup will either elect or take over and promote eligible node to replace it.

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.

Dynamic clustering is also employed as described in Section 3.2 and involves Merge and/or Join functions, which will be triggered based on pre-determined thresholds. This would allow the optimization of the network and better scalability.

4.2 Cross-Domain Communication

We classify domains as either extended or Alien; the former is an extension of the same service, e.g. divisions in the same university, while the latter is an external or anonymous domain. The key difference between the two is the level of trust which will be built through the PS in each domain.

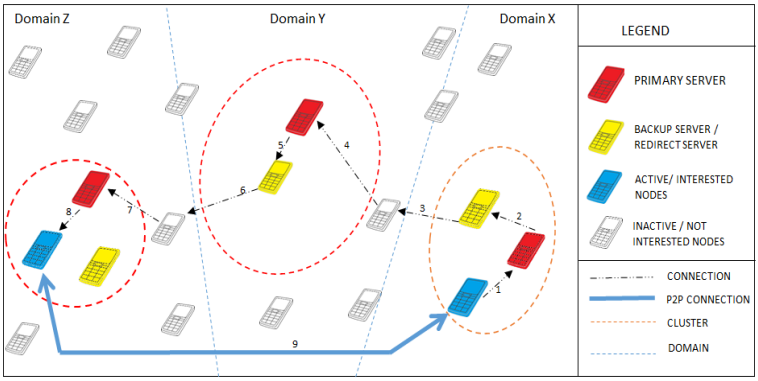

Fig. 2. A cross-domain SIP solution for MANETs

We assume that domains are built using our own solution, such as [16]. We introduce a new BS functionality in order for the BS to act as redirect servers. This would allow the BS to redirect outbound requests, and calculate AUTH. Its reputation builds over time and the local decision whether to either invitations to clients in the cluster or require more authentication points are required (see Equation (1)).

Once domains have been built and communication within clusters in the domains is up and running, subsequent requests from other domains (outbound requests) will be handled as follow:

1. PS authenticates the request using public keys of the initiating PS.
2. Once authenticated, PS will then sign the requests using its private key and forward them to the redirect server (BS). Points will also be gained by the PS.

3. BS authenticates this request using the sender PS's public key. Once authenticated, the AUTH field will be updated in its AOR against the PS who initiated the request. This will trigger the dynamic timer, T.
4. BS forwards the requests to the next functioning PS where the same process will be repeated until the request reaches its intended recipient.
5. Once the PS who holds the record in the location service table of the client who is the intended recipient of the invitation receives the request, will forward the request to its functioning BS without signing the request.
6. BS will then make a decision based on the AUTH field of the request initiator PS.
7. If the request is authenticated, ACK will be sent back to the caller allowing P2P communication between both parties to be established (see Fig. 2).

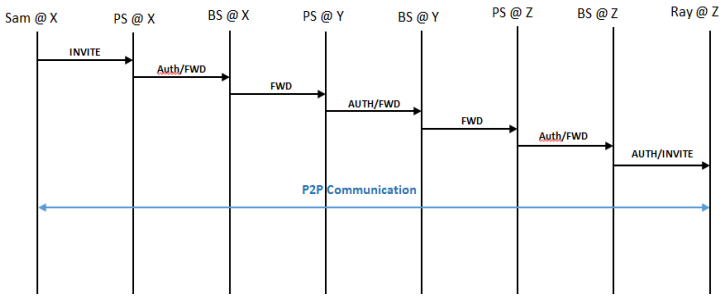

Fig. 3. Call flow through SIP proxy server and backup server

Fig. 3 illustrates a typical call flow, and in this example, user Sam initiatives a request from domain X to another user, Ray, from domain Z, passing through domain Y. The call flow involves the following steps:

1. Sam initiates an INVITE request to call Ray.
2. PS authenticates (Auth) Sam as part of this cluster and domain before signing the request with its private key.
3. PS forwards the message to its functioning BS.
4. BS at domain X labels this request as outbound and forwards it to the next available PS, and in this context, PS at domain Y.
5. PS at domain Y will authenticate the PS at X using its public key and forward it to its BS.
6. BS at domain Y will update its AUTH field using equation (1) and forward the request to the next available PS, and in this context, PS at domain Z.
7. PS at domain Z receives the request and authenticates (Auth) Ray as part of this cluster and domain and forwards the INVITE to its BS.
8. BS at domain Z will then update its AUTH field in its AoR and make a decision on either to forward the request to Ray or not. The decision is made based on the threshold calculated against the points resulted from Equation (1).

9. Once the threshold is achieved and the decision has been made by BS at domain Z, BS forwards the INVITE request to Ray at domain Z.
10. Once an INVITE received by Ray at domain Z, the P2P communication channel will be established between both parties.

Note that if the INVITE requests routes through additional PSs and the involved PS stay online longer, the reputation of the PS involved will be increased. This will result in more eligible or 'trustworthy' PS, and consequently, increasing the scalability of the network. This concept is analogous to passport and visa, where requests are similar to passports, and the more visas the passport holder receives, the more 'international exposure' the individual is (in our context, cross-domain).

5 Discussion

We evaluate our implementation outlined in Section 4 using the following parameters:

- Overhead: The average number of SIP messages received per second.
- Success Ratio: The average rate of invitations successfully delivered to the intended recipient over time.
- Scalability: The performance of the implementation when the number of nodes and area increases.
- Stability: The effect on the service request time when the number of nodes increases.
- 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.

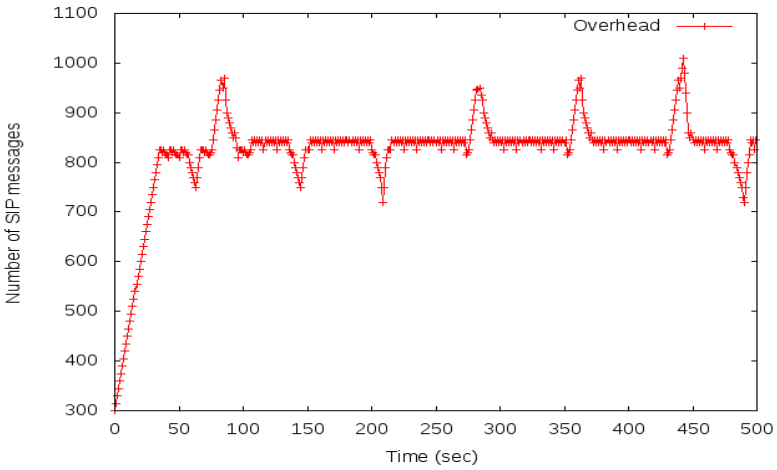

Fig. 4. Number of nodes per cluster over time

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 (i.e. mobility) with time.

Fig. 4 presents the findings of the effect of the number of packets measured in kilobits over the lifetime of the network. As observed in the simulation of the implementation, at the startup of the scenario, the number of SIP management messages increases significantly until it reaches a stable position that ranges between 700 and 1000 messages across the network. This is due to the fact that at the initiation of the simulation, the discovery messages dominate the computational resources. Once the network reaches an 'acquainted' state (i.e. where PSs are familiar with neighboring clusters and domains), the network stabilizes and behaves normally according to the proposed solution. It is also observed that the network might face some what is shown in the figure as peaks and drops. The peaks are justified as an impact of authenticating a new domain which adds up a significant number of nodes to the network allowing the number of SIP messages through the redirect servers to increase, conversely, the drops are justified by un-authenticating a domain which significantly decreases the number of nodes, hence an overall decrease of the number of SIP messages through redirect servers.

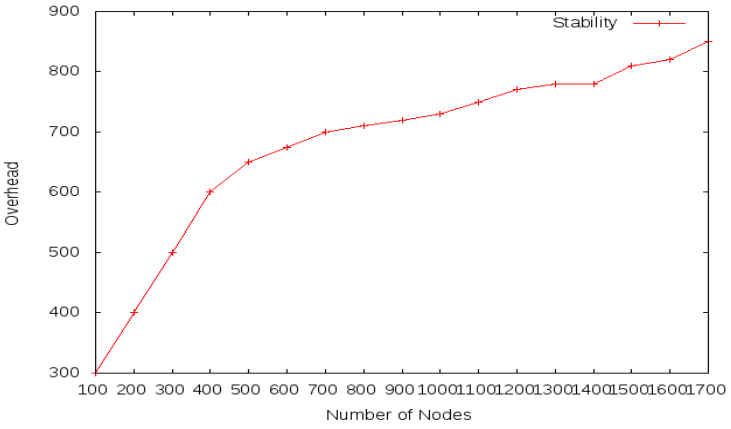

Fig. 5. Stability

As shown in Fig. 5, as the number of nodes increases, the overhead in our implementation remains relatively low – in the range of 100 to 500 nodes. Once the simulations hit the ballpark range of 600 to 1500, the overhead gradually increases with a reasonable delay time. This is due to the restriction that our proposed solution had on the number of messages. This ensures that the success rate is consistent and the system does not degrade over time.

It is also evident in the simulations that the impact on the network is kept to a minimal; the dynamic multi-clustering mechanism in our proposed solution divides the load, resulting in a fair distribution of the load carried by each cluster.

However, once the simulations are 1500 or more, the overhead increases rapidly which produces a significant delay time. This may cause messages to be dropped. This is due to the large number of inbound and outbound messages influenced by the large number of nodes. This limitation will be the subject of future investigation.

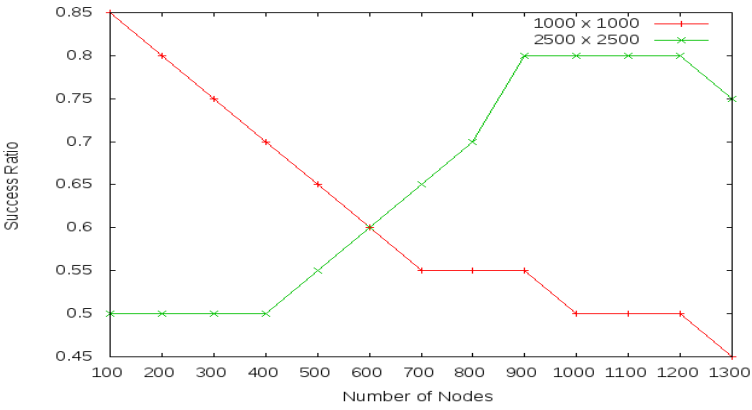

Fig. 6. Scalability (number of nodes against the simulation time)

As shown in Fig. 6, our cross-domain approach has significantly increased the number of participating nodes; addressing one of existing challenging issues. We were able to achieve this by employing a new functionality of the redirect servers and by dividing the network into clusters and domains to evenly share the network load using dynamic clustering across domains in the same domain. The approach is simulated in different terrain areas to achieve an optimized solution. Our simulations suggested that the average success ratio is inversely proportional to the number of nodes for a smaller terrain area for the network layout. On the other hand, our simulations suggested a gradual increase of the average success ratio as the number of nodes increases in a bigger terrain area, from an average starting point of 50% to an average of slightly above 80%. This is due to the impact of the increased number of available routes, which reduces disconnections among cluster and domains. We also remark that the domain can choose not to authenticate and register other domains based on the AUTH equation as the domain may not be stable or is known to be compromised.

As shown in Fig. 7, our cross-domain approach has also been simulated using four different terrain areas. We achieved an average success ratio of 65%-60% for the condensed scenario (i.e. between 500 and 1,800 modes), and 50%-45% for the scattered scenario for the 1,000 m^2 terrain area. For the 1,500 m^2 terrain area, we achieved an average success ratio of 60%-50% for the condensed scenario and 45%-35% for the scattered scenario. In the 2,000 m^2 terrain area, the average success ratio is 50%-45% for the condensed scenario and 35%-30% for the scattered scenario; and for the 2,500 m^2 terrain area, the average success ratio is 45%-35% for the condensed scenario and 30%-25% for the scattered scenario.

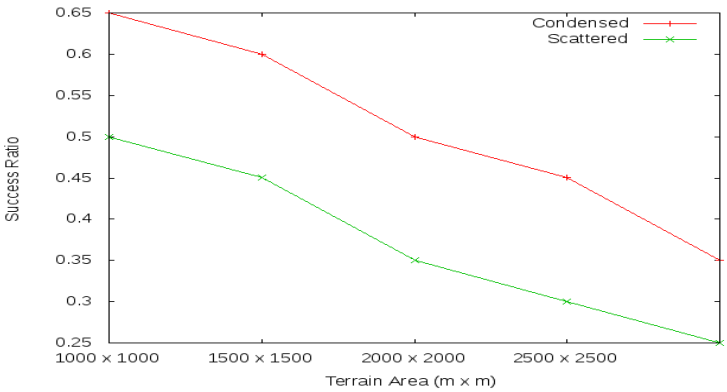

Fig. 7. The impact of terrain area on the success ratio

The simulations indicated that a condensed network results in better performance. This is, probably, due to a higher probability of finding routes and a lower probability of disconnections (i.e. gap between connections). As the number of nodes increases, the success ratio decreases as the increased number of SIP messages would cause a high overhead. Consequently, this leads to a significant delay, which causes the packets to be dropped.

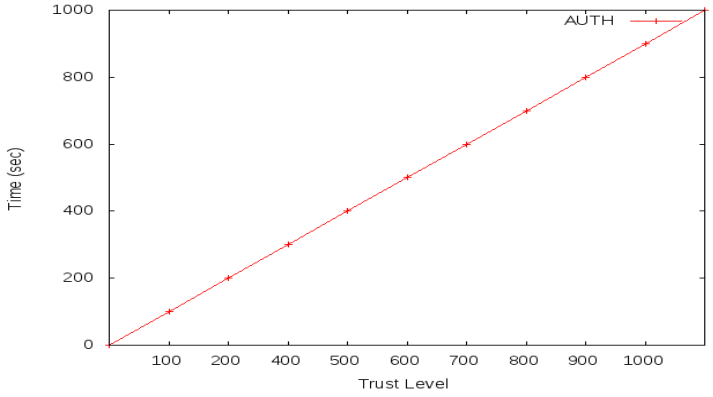

Fig. 8. Reputation

Fig. 8 shows a linear relationship between reputation and time resulting from implementing the equation (1) which ensures a growth of the trust level over time, and points rewarded ensures the most stable servers are preferred and maintain a global list of the authenticated registered entities (i.e. based on number of times the local and global entities were selected).

Table 1. Comparative summary

	Kagoshima et al. [10]	**Leggio et al. [12]**	**Abdullah et. al. [14]**	**Almobaideen et al. [15]**	**Aburumman et al. [16]**	**Our Solution**
Priority	Dynamic	Static	N/A	N/A	Dynamic	Dynamic
Scalability	Up to 10 nodes	Up to 100 nodes	Up to 50 Nodes	Up to 100 Nodes	Up to 350 Nodes	Up to 1500 Nodes
Average number of management packets	*Gradual Increase	*Rapid Increase	*Rapid Increase	*Gradual Increase	Gradual Increase	Gradual Increase
Stability	Stable	Limited	Stable	Limited		Flexible
Overhead	Low	Varies	High	Average		Average

*The results may vary depending on the conditions of the network, which relies on the applied parameters for the simulated network.

We proposed a solution that is able to enhance and overcome issues previously identified in [13], [14] and [16]. In other words, we were able to address the shortcomings associated with scalability without compromising on reliability and security.

Existing approaches (see Table 1) do not generally address security and stability [10], security and scalability [12, 15], and scalability and overhead [14]. Our proposed solution attempts to address these issues; using an improved priority mechanism, we enhance the trust level associated with the functionalities of SIP entities and consequently, enhance the overall security and availability. This allows one to virtually organize and administrate the network in a dynamic way, and across domains.

6 Concluding Remarks

In this paper, we proposed a cross-domain SIP solution for MANETs using dynamic clustering, which resulted in a stable, secure and scalable MANET service. Our proposed solution introduced new functionalities designed to scale across domains, providing an effective way to deal with outbound requests. We demonstrated the utility of our solution by simulating the implementation under different settings, and evaluated using different metrics and parameters.

Future work includes deploying the solution in a university campus involving student and staff mobile participants, which will allow us to evaluate and refine the design.

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. IEEE Press and A John Wiley & Sons Inc. (2004)
3. Alonso, G., Remund, A., Stuedi, P., Bihr, M.: 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., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., Schooler, E.: 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, IETF (2003)
7. Leggio, S., Manner, J., Hulkkonen, A., Raatikainen, K.: Session initiation protocol deployment in ad-hoc networks: a decentralized approach. In: Proceedings of 2nd International Workshop on Wireless Ad-hoc Networks (IWWAN) (2005)
8. Bai, Y., Aminullah, S., Han, Q., Wang, D., Zhang, T., Qian, D.: A novel distributed wireless VoIP server based on SIP. In: Proceedings of International Conference on Multimedia and Ubiquitous Engineering (MUE 2007), pp. 958–962. IEEE (2007)
9. Bah, S.: SIP servlets-based service provisioning in MANETs, Concordia University (2010)
10. Kagoshima, T., Kasamatsu, D., Takami, K.: Architecture and emulator in ad hoc network for providing P2P type SIP_VoIP services. In: Proceedings of IEEE Region 10 Conference (TENCON 2011), pp. 164–168. IEEE (2011)
11. Alshingiti, M.: Security Enhancement for SIP in Ad Hoc Networks, Carleton University (2012)
12. Leggio, S., Miranda, H., Raatikainen, K., Rodrigues, L.: SIPCache: a distributed SIP location service for mobile ad-hoc networks. In: Proceedings of Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services (MobiQuitous 2006), pp. 1–4. IEEE (2006)
13. Aburumman, A., Choo, K.-K.R., Lee, I.: Nomination-based session initiation protocol service for mobile ad hoc networks. In: Proceedings of 22nd National Conference of the Australian Society for Operations Research (ASOR 2013), pp. 149–155. The Australian Society for Operations Research (2013)
14. Abdullah, L., Almomani, I., Aburumman, A.: 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)
15. Almobaideen, W., Kubba, N., Awajan, A.W.: FCSIP: fuzzy and cluster based SIP protocol for MANET. In: Proceedings of International Conference on Next Generation Mobile Apps, Services and Technologies (NGMAST 2014), pp. 169–174. IEEE (2014)
16. Aburumman, A., Choo, K.-K.R.: A domain-based multi-cluster SIP solution for mobile ad hoc network. In: Proceedings of International ICST Conference on Security and Privacy in Communication Networks (SecureComm 2014). Springer (2015)
17. Azfar, A., Choo, K.-K.R., Liu, L.: Android mobile VoIP apps: A survey and examination of their security and privacy, Electronic Commerce Research (In press)
18. Azfar, A., Choo, K.-K.R., Liu, L.: A study of ten popular Android mobile VoIP applications: are the communications encrypted? In: Proceedings of Annual Hawaii International Conference on System Sciences (HICSS 2014), pp. 4858–4867. IEEE (2014)
19. Imgraben, J., Engelbrecht, A., Choo, K.-K.R.: Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users, Behaviour & Information Technology **33**(12), 1347–1360 (2014)