International Journal of Computer Science and Applications,
©Technomathematics Research Foundation
Vol. 12, No. 1, pp. 134 – 147, 2015

A NEW AUTHENTICATION SCHEME FOR SIP REGISTRATION IN A MANET ENVIRONMENT

AICHA AIT HACHA, SLIMANE BAH and ZOHRA BAKKOURY

AMIPS Research group, Ecole Mohammedia d'Ingénieurs (EMI), University Mohammed V
Rabat, Morocco
a.aithacha@gmail.com, slimane.bah@emi.ac.ma and Bakkoury@emi.ac.ma

SIP identity theft is a big issue which can be exploited by attackers to gain control of network resources and conduct fraud using a stolen legitimate identity. This concern is more challenging when it comes to MANET (Mobile Ad-hoc Network) which is more threatened by eavesdropping and impersonation due to its dynamic and wireless open environment. In this paper, we propose a new authentication scheme as a part of SIP Registration to address this problem. This is achieved by the use of smart antennas and hash chaining during password provisioning phase. We propose that each SIP node provisions a set of her well reputed neighbors (which are determined by some Reputation based system) with a one-time password and the associated hash function. These neighbors with good reputation will act later as the node's witnesses to prove the SIP Identity to the Registrar during the SIP Registration.

Keywords: Authentication; hash chain; MANET; Reputation Based Systems; Smart Antennas; SIP Registration.

1. Introduction

By way of introduction, we can define a MANET network as a collection of mobile nodes which share temporarily the same wireless medium and where each node performs due the lack of a fixed infrastructure, a part of the whole network functionalities such as routing, services and security tasks in a collaborative way. This kind of network called MANET has gained the interest of the scientific community since the mid-'90s in furtherance of the ubiquitous computing concept, driven by the ease of its deployment and administration as compared to the conventional networks, allowing in this manner to sidestep the heavy investment in infrastructures. The aforementioned characteristics of MANET make it the most suitable network for emergency services, disaster recovery and battlefield communications. However, the use of MANET can be extended to afford new commercial applications and new business opportunities, provided to develop the economic model and the strategy related thereto. This also requires providing much effort to design and implement multimedia and advanced services over MANET and it becomes inconceivable to design such services without using SIP [Rosenberg, et al., (2002)] (Session Initiation Protocol). This signaling protocol was selected for IMS [Martin, (2005)] (IP Multimedia Subsystem) which gives it a grand momentum. SIP deals initially with session establishment and control, it also allows terminal to negotiate session properties in order to provide services such as basic voice, presence, video conference, messaging and so on...And as like any kind of networks, SIP over MANET has its requirements and constraints in terms of routing, QoS and Security. In this paper, we focus on the security aspect and treat specifically the authentication issue for SIP over MANET. We propose a new authentication scheme that takes into consideration MANET challenges and defeats the most likely and common attacks in such environment. As a division to this paper, we take into consideration the major highlight to begin with an overview of the existing authentication solutions whether in traditional networks or MANET ones. Then, we come to spot the light on our new authentication scheme and its advantages compared to these existing solutions. Finally, we discuss our future directions.

2. Related Work

The authentication is the procedure used by the user to confirm her identity and ensure that she is the one who is claiming to be. It's obvious that authentication is a compulsory security concept and a must for trust establishment and Network protection against unauthorized access or identity impersonation. Different methods can be used to achieve authentication purpose and are described in the following sections.

2.1. *View of authentication methods in traditional network:*

The Password based authentication method is the simplest form of authentication but it's vulnerable to many types of threats including eavesdropping, password guessing such as brute force attack or dictionary attack, hybrid attack and cracking using for example the rainbow tables. To mitigate the aforementioned weaknesses and enhance the password method security, the one-time password (OTP) authentication is proposed. Lamport has proposed in 1981 a tremendous one time password scheme in which the secret password is only stored in the user side, moreover intercepting network exchanges cannot reveal this secret. This scheme is based on a sequence of computations performed on the secret in the user side: $\{x, F(x), F^2(x), F^3(x), ..., F^n(x)\}$ where x is a random value chosen by the user, n is the number of authentications, and F is a one way function as hash function. The OTP authentication process is described below:

On the onset, the server must be provisioned by $F^{n}(x)$.

For her first time authentication, the user sends $F^{n-1}(x)$ as her first one-time password. Then, the server simply applies the function f(x) to the received value and checks if it finds the first provisioned value. For the ith authentication, the user sends $F^{n-i}(x)$ then the server verifies the user identity by computing $F(F^{n-i}(x))$ and checks if it falls on the previous value $F^{n-i+1}(x)$. The main shortcoming of this method is the high amount of needed computation if the number of authentication 'n' is large thus the determination of this number requires a particular attention [Groza and Petrica, (2005)].

Another famous authentication approach is the public key certificated based, which uses a digital signature for the binding of a public key with the appropriated identity. In that scheme, the user signs her message with a digital signature that has the property to be computed based on her private key, and then the receiver checks the sender's identity using the corresponding public key. Many existing protocols make use of the public-key authentication such as TLS and DTLS. For instance, TLS uses to perform authentication task the public-key procedure coupled with MAC verification. The MAC (Message authentication code) is a cryptographic checksum which is computed based on the message to be sent and a secret key shared between the sender and the receiver. When the receiver receives the messages and the MAC, it performs the same computation to verify the message integrity and the source authentication at once. This procedure assumes that the secret key is securely exchanged between the sender and the receiver; it's also vulnerable to some attacks like brute force key search and generic forgery attack [Handschuh and Preneel, (2008)].

One of the most well-known authentication protocols is Kerberos, which was designed at MIT's Project Athena [Bryan, (1988)]. Its goal is to ensure the authentication of the whole entities in the network (clients or servers) based on a trusted third party, thus it soothes the resource servers from the management authentication task. The Kerberos protocol relies on client/server architecture and introduces for the first time the concept of “the ticket” used by the resource server to identify the client. The main drawback of Kerberos is its dependency on a centralized entity which is the KDC (Key Distribution Center), i.e. the security of the entire network will be affected if the KDC is compromised.

Actually, there are several other authentication approaches that include inter alia Multi-Factor Mechanisms which requires that the user provides two or more validated authentication factors in order to be authenticated: a knowledge factor, a possession factor and an inherence factor. Most of the Multi-Factor Authentication methods such as tokens, SMS, and telephone based methods are vulnerable to MitM attack. Another concept is the challenge-response authentication which consists of the presentation of a challenge to the user which has to provide the valid response in order to be authenticated. Many methods meeting this paradigm are deployed currently such as HTTP Digest Authentication, the plain SASL mechanism, the CRAM-MD5 SASL mechanism; and so on…Each one of these mechanisms presents a set of vulnerabilities, the plain SASL for instance, is vulnerable to eavesdropping and impersonation unless TLS is combined with it.

In order to overcome the problems faced by the traditional Challenge Response Authentication Paradigm, [Newman, et al., (2010)] proposes a Salted Challenge Response Authentication Mechanism (SCRAM) which depicts the binding of the past Challenge Response Authentication Mechanism and a security layer like TLS. SCRAM defeats eavesdropping impersonation by the use of salted passwords, provides mutual Authentication and secures transport of authorization identities from the client to the server. Without the use of an external security layer, SCRAM cannot defeat eavesdropping.

The following section tackles the SIP Authentication methods.

2.2. *SIP authentication*

SIP specifications [Rosenberg, (2002)] recommend the use of existing security mechanisms instead of developing new ones. SIP security can be provided end-to-end or hop by hop, several mechanisms can be implemented for that including HTTP Digest Authentication, TLS/DTLS [Dierks, (2008)], IPSec [Kent, (2005)] and S/MINE [Ramsdell, et al., (2010)]. HTTP Digest Authentication is a challenge-response mechanism used by the client to prove its identity to the server without sending its password. The principle is that the user applies a hash function to the password and a random value (called a nonce) and then sends this digest to the server, which will perform the same calculation and will authenticate the client if it falls on the same result. To illustrate, figure 1 and 2 show the IMS registration call flow based on HTTP Digest Authentication.

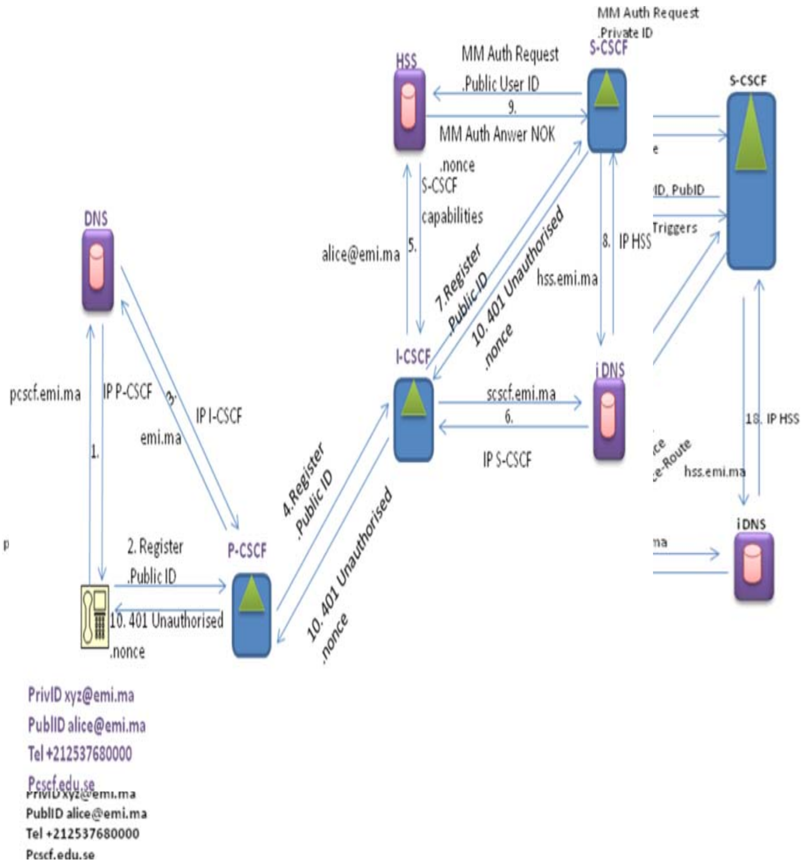

Fig. 1. First step in IMS SIP Registration

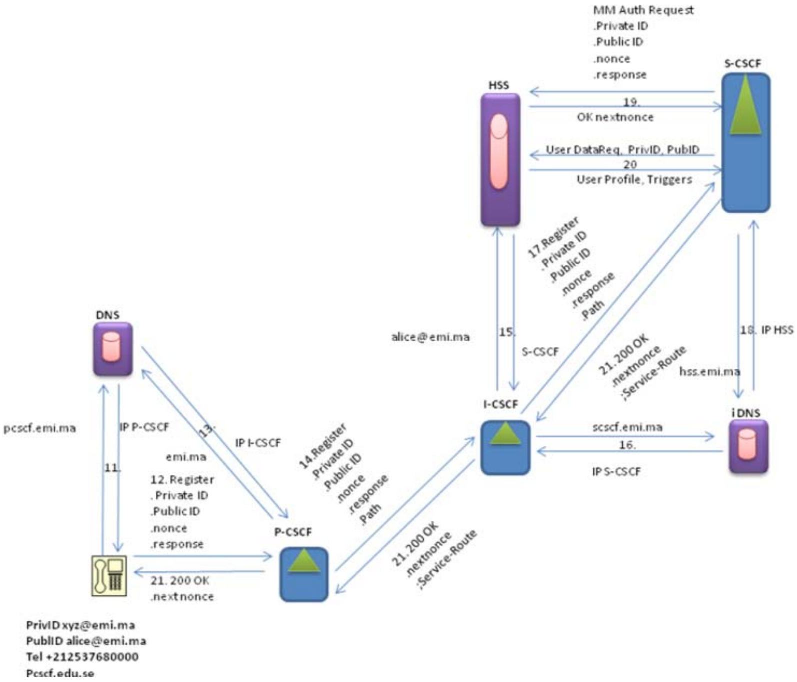

Fig. 2. Second step in IMS Registration

HTTP Digest Authentication mechanism [Franks, (1999)] is more secure with regards to Basic Authentication in which the user sends its password in clear text to be authenticated by the server, but still suffer from several minimum level of protection for the undermentioned shortcomings:

- the use of HTTP Digest Authentication requires a pre-provisioning of user data at the server;
- it’s vulnerable to the MitM bid-down attacks;
- it’s not as secure as strong authentication protocols like Kerberos or public-key based;
- it also offers a limited integrity of merely the message body, thus in SIP headers are important and need to be protected....

S/MIME is also one of the recommended standards by the SIP RFC 3261 to secure SIP communications; it provides inter alia the authentication service by the use of public-key certificate. It’s used to handle the replication of SIP header fields at a MIME body. This ensures authentication by signing replicated header fields to verify the identity of the issuer. RFC 3261 proposes to replicate all header fields at the MIME part which causes some problems: the content can be modified by the intermediate SIP proxies which can lead to the receiver confusion; it will be unable to distinguish a legal change from a malicious one. Also, SIP messages will be very large to be treated or transported.

Concerning TLS, its Handshake Protocol part provides authentication based on certificate exchange. Note that TLS operates only over TCP, that's why DTLS (Datagram TLS) was designed to cope with this and operates over unreliable transport protocol such as UDP.

IPsec is also recommended by SIP specifications. This protocol is often partially understood due to its intricacies. It provides terminal authentication and not user authentication. IPsec adds a significant overhead through the use of tunnel mode (by adding a new IP header). Also, the IPsec transport mode is not compatible with the use of multiple proxies and NAT because these components change different field's packet, which attains data integrity and leads to the IPsec packet discarding.

The authors of the article [Cha and Choi, (2007)] propose to determine which of the existing security protocols TLS, DTLS and IPsec, have less impact on SIP performance. To do this, they propose to calculate and compare the call setup time for different combinations of security protocols and transport protocols (TLS / TCP, DTLS / SCTP , DTLS / UDP, TLS / SCTP, IPsec / UDP IPsec / TCP and SCTP / IPsec). According to this study, the TLS/SCTP combination with the period of the greatest call setup is the least efficient. The SCTP multi- streaming chooses to avoid any blocking TLS messages due to HOL (Head -of- Line). In this case, SIP must open as many sessions as there are TLS/SCTP streams which lead to network congestion, given the large number of messages required to establish TLS sessions.

This large number of exchanges will also increase the call set up time. While the combination TLS / SCTP is the least efficient, combinations based on UDP as DTLS / UDP and UDP / IPsec allow very optimized call set up compared to other combinations. But it should be noted that the use of the UDP will lead to a lack of congestion control and therefore a greater failure rate of call setup.

2.3. *Authentication in MANET*

By definition of a MANET network, critical network functions (as switching, routing and security) have to be performed by MANET nodes themselves. Yet, these nodes cannot be trusted to execute correctly these functions due the fact that MANET is an open environment which is characterized by the lack of PKI, selfishness, as well as its vulnerability to several attacks such as eavesdropping, masquerading and so on...In terms of cryptanalysis, some attacks can be performed through public key replacement or by compromising private keys. This makes Key management in MANET one of major issues which have aroused the scientific community interest. Several issues are blown out from private key management like the key setup problem and public key management [Dini, (2008)].

To deal with public key management issue, [Luo and Lu, (2000)] and [Zhou and Haas, (1999)] propose a robust authentication service which distributed keys among the available nodes in the network. It makes use of what we call "Threshold cryptography" that cuts any secret into several pieces and thus, any malicious node has to compromise many nodes before taking control of this secret.

It has been suggested to build a trust aggregation in such a way that the corruption of some node will not impact the overall network. Its challenge not only lies in this aggregation construction but also in its security maintenance in spite of the dynamic topology changes of the network. Due to the lack of a fixed infrastructure in MANET, nodes can play the role of certificate authorities. The concept of trust distribution can be applied via the replication of the key on all nodes which opposes the aggregation safety by increasing the likelihood of secret disclosure; hence the idea of "secret sharing" [Shamir, (1979)] between nodes has arisen. As aforementioned, based on polynomial interpolation, the secret is divided into "n" parts and distributed to "n" nodes in such a way that at least "t" parts t<=n, must be gathered to rebuild the key. To enforce this security measure, we adopt what we call "Periodic share refreshing" method to refresh periodically the key parts. For shares calculation, they construct a t-1 degree polynomial where the constant coefficient represents the secret and other coefficients are generated randomly as:

$y=f(x)=a_{t-1}x^{t-1}+a_{t-2}x^{t-2}+...+a_1x+S$. For $t\leq n$, each share is a pair of (xi,f(xi)) and xi is different from 0. By means of Lagrange interpolation, we can determine the polynomial using any combination of t shares and then can obtain the secret "S". The above procedure using Shamir's scheme supposes that there is a trusted and centralized dealer in the network which performs this computation and distributes securely share among nodes. Pedersen scheme [Pederson, (1991)] removes the need of this dealer, and its task is done collectively by the group members. This is what we call JSS (Joint Secret Sharing). Suppose that there are "n" members in the group (M1, M2,…,Mn), it's assumed that all members have agreed on a prime number "p".

(1) Each member Mi chooses a polynomial fi(x) of a degree t-1, fi(0)=Si.

(2) Mi calculates shares for all the other peers Mj and securely sends them.

(3) Each Mj calculates her share sj as the sum of all the received shares from the other members sj=∑sij.

In order to detect incorrect secret shares that can be generated by malicious nodes, [Feldman, (1987)] proposes VSS (Verifiable Secret Sharing) to verify the shares. Many papers have proposed to use threshold cryptography to achieve authentication purpose in MANET but do not properly address issues related to MANET such as the dynamic change of threshold proportionally to the group size [Narasimha, et al., (2003)].

[Apkun; Buttyan and Hubaux, (2002)] is inspired by PGP to propose another approach for authentication and security of communications in self-organized mobile ad hoc networks bypassing the need of a certification authority or a centralized server. According to this approach, key authentication is done in the following way:

(1) the user u can verify directly the first certificate of the chain using a public-key that she holds and trusts

(2) for the following certificates, each one can be verified by the public-key contained in the previous certificate in the chain.

Each node u has a local certificate repository with some certificates of trusted neighbors. When she wants to authenticate the public-key of some other node v, both merge their local certificate repositories and v looks for a certificate chain to v.

[Pirzada and Mc Donald, (2004)] presents Kaman (Kerberos assisted Authentication in Mobile Ad-hoc Networks) which is an authentication service based on Kerberos protocol and designed to suit MANET environment. This scheme inherits Kerberos features and advantages such as mutual authentication, prevention of forgery identity and replay attack detection. It relies on multiple Kerberos servers which replicate periodically or on-demand hashed password data bases with each other.

2.4. *Critical overview of MANET related work:*

Several researches [Boonkrong and Bradford, (2004)], [Irshad, et al., (2008)] have proven that the existing authentication protocols don't suite the MANET network or are even not applicable in such environment. It's obvious that traditional methods such as Identity-based cryptography, involving a trusted third party, are not applicable in MANET because it is against the very essence of this kind of network which consists of flexibility and scalability. This kind of methods requires less traffic as compared to Threshold cryptography, described in the section above. It's worth to mention that the Threshold Cryptography has the advantage to circumvent the single point of failure problem but in the other hand, it requires more overhead and more processing. In addition, there is a risk to not be able to recover the key if there are less available nodes than the needed number “t” (see the section above).

Otherwise, the aforementioned KAMAN [Pirzada and Mc Donald, (2004)] scheme which is developed specifically to provide MANET authentication has its own vulnerabilities and drawbacks. It doesn't give details about the initialization configuration and how the first repository is securely provisioned by hashed passwords of network nodes. It's not even secure against eavesdropping of the session key exchange and servers are not even trustworthy.

Concerning the aforementioned framework proposed in [Abdala and Al-Zuhairy, (2013)] which is similar to PGP, its authors recognized that it gives only probabilistic guarantees [Hubaux, (2001)]. To detect dishonest users which issue false certificates, this scheme relies on some sort of authentication metrics which are not sufficient to measure the effect of dishonest nodes on the public-key distribution system.

Moreover, this scheme does not address the mobility and dynamic aspects of MANET and provides no means to prevent dishonest user from issuing false certificates.

3. The proposed Authentication scheme

In this section, we describe our new authentication scheme for SIP Registration in MANET. This scheme has the property to suit the MANET infrastructureless nature and defeats eavesdropping, replay and impersonation attacks while discouraging selfishness and allowing location based services in MANET by the use of smart antennas. Our scheme relies on different techniques to protect SIP node credentials and ensure the authenticity of the registered node. One of these techniques is the use of smart antennas instead of omnidirectional ones. It's worth to mention that our choice of the use of this kind of smart antennas is a well-thought out security measure, as any malicious node which project to sniff (eavesdrop) credentials, needs to be positioned at the same time at different positions, precisely the accurate positions of the different beams which are sufficiently narrow and pointing to the selected neighbors. Smart Antennas estimate the location of the receiver to increase capacity and decrease interferences by directing power to the accurate position of the receiver instead of disseminating power in all directions. Many researches have focused on the use of smart antennas in MANET in terms of MAC protocols and Direction of Arrival (DOA) estimation. [Abdala and Al-Zuhairy, (2013)] proposes to use a position-based routing protocol using GPS to find the accurate position of MANET nodes and estimate DOA. The use of smart antennas in MANET is a circumspect measure that ensures physical layer security by sending in a unidirectional manner the information to the intended receiver and preventing interferences as well as eavesdropping.

Our new authentication scheme also utilizes some reputation system which allows the user to select her guarantors among good reputed neighbors. This astute measure enhances security by restricting the choice of node witnesses to cooperative nodes. These witnesses have to confirm the node identity to the registrar. By the use of reputation based system, we avoid that the user and her Registrar interact with selfish and misbehaving nodes which may not take part in the registration procedure or may disturb the smooth conduct of it. Concerning the possible reputation based schemes to be used by our scheme; they are classified based on their monitoring component [Abbas; Merabti, and Jones, (2010)] Passive acknowledgment monitoring techniques as watchdog or Pathrater techniques, and Active acknowledgment monitoring techniques that use explicit acknowledgments. For instance, the watchdog technique is the simplest reputation based system. It consists on a process running on each node that maintains a reputation table to record the reputation of one hop neighbors. Every time a source S sends a packet to the destination node D via intermediate node, S holds a copy of the packet in memory until it overhears (in promiscuous mode) the same packet forwarded by the intermediated node before time T expires. The node S increases the reputation weight of the one hop neighbor when it is confirmed that it has forwarded its packet, and decreases it otherwise after a time-out period.

Our scheme is divided into three separated processes: provisioning, registration coupled with authentication and re-provisioning.

3.1. *Assumptions:*

In order to perform the undermentioned authentication scheme, we assume that:

- Links are supposed bidirectional;
- The environment is running a Reputation based Software [Abbas; Merabti, and Jones, (2010)];
- Each node supports a set of different hash functions;
- Antennas are adaptive;
- Nodes are moving with a low speed.

3.2. *Provisioning Phase:*

In general, SIP provisioning is the process of communicating and storing the SIP password in the server. Note that SIP standard recommends to store digests of passwords rather than storing the plaintext passwords. The novelty of the proposed provisioning process lies in its robustness to eavesdropping and replay attacks by applying a random hash chain and communicating in a unidirectional manner an OTP to a set of well-reputed neighbors which are selected randomly. Then the password or its digest storage becomes needless in our case, which prevents rainbow table attack. The provisioning phase consists of the following steps:

(1) Each SIP node N in our MANET network chooses a random set of its first hop neighbors {M1,…,Mn} with a good reputation. By this way, we are pretty sure that the chosen nodes will cooperate correctly in the registration phase,

(2) N makes use of one of the existing location position algorithms [Abdala and Al-Zuhairy, (2013)] used by smart antennas to locate its neighbors,

(3) Note that each node N maintains an ordered list of supported hash functions (SHA, MD5...). N chooses randomly for each node of Mia hash function Hi and the number of expected iterations “p”.

(4) N communicates H_i^p(password) to each node of its chosen neighbors, applying the hash chain technique aforementioned (in section A of paragraph II). These Digests are sent to neighbors using unidirectional smart antennas instead of the use of omnidirectional antennas.

(5) N broadcasts the set of the selected nodes Mi to the whole network.

(6) Note that nodes Mi will serve later as Node’s N guarantors or witnesses to prove her identity to the registrar.

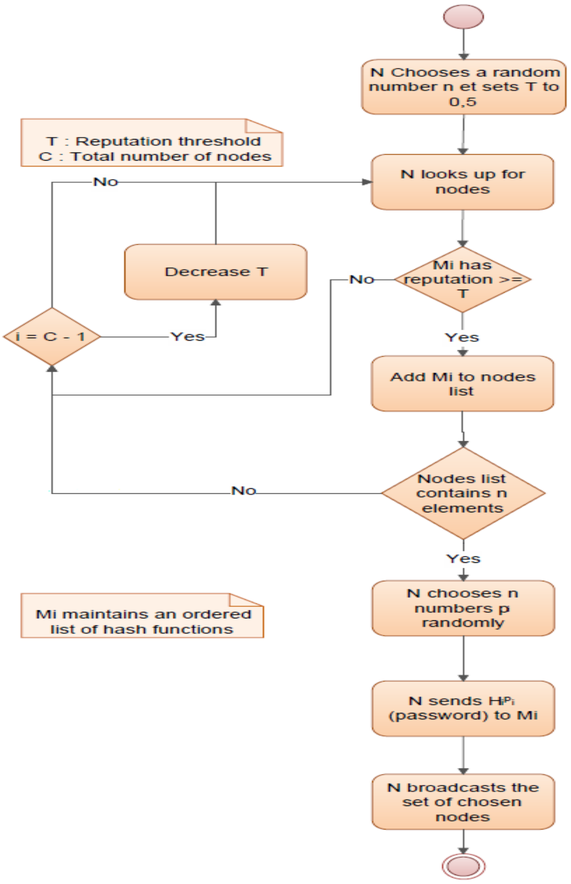
N Chooses a random number n et sets T to 0,5
T : Reputation threshold
C : Total number of nodes
No
N looks up for nodes
Decrease T
No
Mi has reputation >= T
i = C - 1
Yes
Yes
Add Mi to nodes list
No
Nodes list contains n elements
Yes
Mi maintains an ordered list of hash functions
N chooses n numbers pi randomly
N sends HiPi (password) to Mi
N broadcasts the set of chosen nodes

Fig. 3. Provisioning phase

3.3. *Authenticated Registration Phase*

The authors in [Wongsaardsakul, (2010)] propose a new P2P framework that makes use of DHT table (Distributed Hash Table) to distribute SIP object identifiers over MANET and perform fast resources lookup. Each peer stores objects with given keys. DHT table is created and updated in real-time using the routing protocol. For SIP registration, the aforementioned scheme consists of the following call flow:

(1) N takes its SIP URI and hashes it; it obtains the Object ID (which is the hash of SIP URI);

(2) then it uses the DHT table (continuously updated using the routing protocol) to find a peer whose Node ID is the closest to the Object ID;

(3) N then forwards the SIP REGISTRAR message to that peer.

As for IMS Registration, we coupled authentication with SIP Registration procedure based on the aforementioned framework. Our new authentication scheme consists of the following steps:

To start registration, N performs the registration procedure described above to find the appropriate Registrar;

If N is not authenticated, the Registrar answers with a 403 FORBIDDEN;

N sends its digests to M_i according to the hash chaining scheme, using for each M_i the chosen hash function H_i during the provisioning phase. Then according to the hash chaining scheme, the digest initially sent to each node M_i for first registration is H_i $^{p-1}$(x);

M_i applies H_i to the digest and checks if the result matches H_i ^{p}(password). If so, N is authenticated. Then M_i nodes relay the SIP REGISTER Message to the Registrar (selected based on the aforementioned framework). By this way, nodes M_i are just like N witnesses to prove N identity to the Registrar.If digests are incorrect, the node N (the binding of the SIP URI and MAC address) is denied from the network for a certain time. (Note that Step 4 requires some changes in the header of the SIP REGISTER Message).

Then the registrar answers the authenticated with a 200 OK.

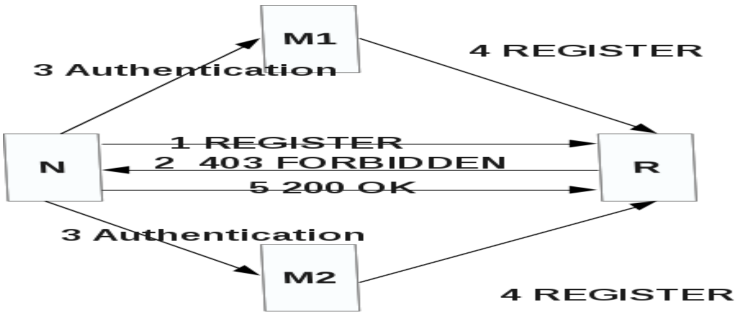

Fig. 4. Authenticated Registration phase

3.4. *Re-provisioning phase*

This phase consists on selecting a new hash function and a new number "p" of iterations to perform the aforementioned provisioning steps all over again.

- Apart from the need of a periodic re-provisioning routine to refresh authentication digests, the re-provisioning is triggered by the following events:
- if a node of the selected neighbors Mi is no longer in the routing table of N,
- if Reputation weight of one of the selected neighbors Mi falls under a given threshold,
- The Registrar is no longer in the routing table of Mi.

The following diagram depicts the re-provisioning process:

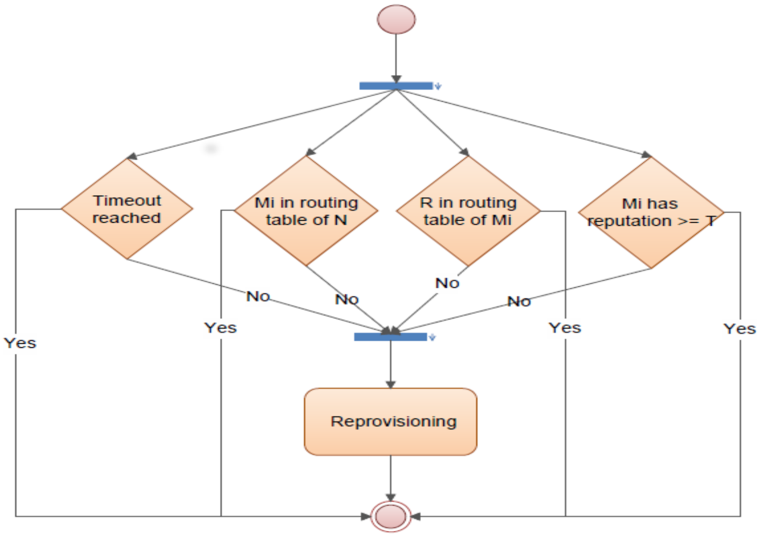

Fig. 5. Re-provisioning phase

We don't purport that our scheme requires less processing and overhead compared to other approaches but our approach kills two birds with one stone, in other terms we try to achieve security and permit the location based services in MANET using the same amount of processing and overhead. As a use case of this scheme, we utilize it during to SIP registration to achieve SIP agent authentication in MANET.

4. Conclusion and Future Directions

This article has introduced a new authentication scheme for SIP Registration on the basis of some techniques such as the use of smart antennas, hash chaining and reputation based system, in order to suit MANET idiosyncrasies and enforce security. The described solution is against eavesdropping, replay attacks, impersonation and selfishness.

Compared to public-key authentication based approach in MANET, the suggested method requires less computation for authentication materials. But in the other hand, it requires additional ones to perform the position location which can be also exploited for other purposes than security (for instance, to implement location based services). Moreover, the hardware needs to be changed to replace the omnidirectional antenna with smart ones. Our future work will secure the choice of the registrar now that none of existing current researches take into consideration security criteria for the SIP Registrar selection. We will also give more details about the used position location algorithm and study our system performance through a simulation.

References

Abbas, S.; Merabti, M.; Llewellyn-Jones, D. (2010): "A Survey of Reputation Based Schemes for MANET," in The 11th Annual Conference on the Convergence of Telecommunications, Networking & Broadcasting (PGNet 2010), Liverpool, UK.

Abdala, M. A.; Al-Zuhairy, A. K. (2013): Integration of Smart Antenna System in Mobile Ad Hoc Networks", International Journal of Machine Learning and Computing, Vol. 3, No. 4.

Apkun, S. C.; Buttyan, L.; Hubaux, J. P. (2002): Small Worlds in Security Systems: an Analysis of the PGP Certificate Graph". In: New Security Paradigms Workshop, Norfolk, VA.

Boonkrong, S.; Bradford, R. (2004): Authentication in Mobile Ad Hoc Networks, In Proceeding of the 1st Thailand Computer Science Conference, pp. 202–207.

Bryan, B. (1988): Designing an Authentication System: A Dialogue in Four Scenes, Massachusetts Institute of Technology.

Buttyan, L.; Hubaux, J. P. (2002): Report on a Working Session on Security in Wireless Ad Hoc Networks, Mobile Computing and Communications Review, vol.6, no.4.

Cha, E.; Choi, H. (2007): Evaluation of Security Protocols for the Session Initiation Protocol. In Proceedings of 16th Computer Communications and Networks, ICCCN

Dierks, T. (2008): The Transport Layer Security (TLS) Protocol Version 1.2 , (RFC 5246).

Dini, G. (2008): Security in Ad-hoc Networks. University of Pisa, Italy.

Feldman, P. (1987): A practical scheme for non-iterative verifiable secret sharing. In FOCS.

Franks, J. (1999): HTTP Authentication and Digest Access Authentication (RFC 2617).

Groza, B.; Petrica, D. (2005): One-time passwords for uncertain number of authentications, in Proceedings of 15th International Conference on control systems and computer science CSCS15.

Handschuh, H.; Preneel, B. (2008). Key-Recovery Attacks on Universal Hash Function based MAC Algorithms, In: Wagner, D. (ed.)CRYPTO.

Hubaux, J., et al. (2001): The Quest for Security in Mobile Ad Hoc Networks. In Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobileHoc), CA, USA.

Irshad, A., et al. (2008): Security Enhancement in MANET Authentication by checking the CRL status of Servers, Springer-Verlag, SERSC-IJAST, DEC.

Jung, E.; Gouda, M. (2004): Vulnerability Analysis of Certificate Graphs.

Kent, S. (2005): Security Architecture for the Internet Protocol, (RFC 4301).

Luo, H.; Lu, S. (2000): Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks, Technical Report TR-200030, Dept. of Computer Science, UCLA.

Martin, M. G. (2005): Input 3rd-Generation Partnership Project (3GPP) Release 5 Requirements on the Session Initiation Protocol (SIP).

Michiardi, P. (2008) : Coopération dans les réseaux ad hoc : Application de la théorie des jeux et de l'évolution dans le cadre d'observabilité imparfaite, Institut Eurecom France.

Narasimha, M., et al. (2003): On the utility of Distributed Cryptography P2P and MANETs : the Case of Membership Control", Proc. IEEE ICNP.

Newman, C., *et al.* (2010): Salted Challenge Response Authentication Mechanism (SCRAM) SASL and GSS-API Mechanisms, (RFC 5802).

Pederson, T. P. (1991): A threshold cryptosystem without a trusted party. In EUROCRYPT.

Pirzada, A. C.; Mc Donald, (2004): "Kerberos Assisted Authentication in Mobile Ad-hoc Networks", ACSC '04 Proceedings of the 27th Australasian conference on Computer science - Volume 26, Pages 41-46.

Ramsdell, B., *et al.* (2010): Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2, (RFC3851).

Rosenberg, J., *et al*. (2002). SIP: Session Initiation Protocol (RFC 3261).

Shamir, A. (1979): How to Share a Secret, Communications of the ACM, vol. 22, no.11.

Wongsaardsakul, T. (2010): P2P SIP over mobile ad hoc networks, Ph.D. dissertation, Dept. Telec. SudParis, Paris.

Zhou, L.; Haas, Z. J. (1999): Securing Ad Hoc Network, IEEE Network.