A Framework for Anonymous Communication in MANETs based on Access Control and Authenticated Key Agreement

Ehab E. Zakaria
Faculty of Computer Science
MSA University
Giza, Egypt
e-mail: ezakaria@msa.eun.eg

Haitham S. Hamza Imane A. Saroit
Faculty of Computers and Information Sciences
Cairo University
Cairom Egypt
e-mail: hhamza@fci-cu.edu.eg, i.saroit@fci-cu.edu.eg

***Abstract*—Mobile ad hoc networks (MANETs) are finding ever-increasing applications in both military and civilian systems owing to their self-configuration and self-maintenance capabilities. Communications in battlefields and disaster recovery are other examples of application environments. Many of these applications are security sensitive. As a result, security in MANETs has recently been drawing much attention. The vast majority of existing solutions that provides security services for MANETS does not take into consideration the need for authentic access control mechanism as a first line of defense to ensure that only the eligible nodes are involved. In this work, we propose an anonymous communication scheme that is based on an efficient access control mechanism with authenticated key establishment. Besides service integration offered by this framework, simulations and analysis showed that the proposed solution enhance quality of service (QoS) level compared to the existing approaches that aims to provide only access control or anonymous services separately. With a similar or a lower cost, our integrated approach enhanced MANET security and performance in comparison with other related proposals.**

Keywords—MANET; Anonymous communication; Access control; Identity-based cryptography

I. INTRODUCTION

Mobile ad-hoc networks (MANETs) are an ideal technology to deploy spontaneous wireless infrastructureless networks, either for military or civilian applications.

Throughout recent years, MANETs have gripped a lot of attention due to its dynamic nature to establish wireless networks of mobile nodes and wireless routers. The key advantage of ad-hoc networks is that the knowledge about network topology is not necessary and even more it's not necessary to have an infrastructure. Without any centralized entity ad-hoc networks are able to operate in an autonomous and spontaneous manner. Also all the required network modifications will be done in a self-configurable way.

In order to have a proper function for a mobile ad-hoc network and achieve cooperation among all networking nodes, it is necessary to limit network access of packet forwarding and routing to righteous nodes and reject access from misbehaving nodes. However, the network access protocols commonly used in traditional infrastructure-based networks are not applicable in MANETs due to the lack of fixed infrastructure, frequent changes in topology and node membership, and finally due to the potential attacks from adversaries inside the network itself [1]. This situation enforces the need to develop different strategies that suit MANET architecture in order to deploy an efficient access control mechanism.

Also, the privacy of communication and sensitive information has become a serious issue on the Internet. Encryption schemes shield the contents of communication, but do not hide the fact that two users are communicating. In many situations, users may need to make their communication anonymous. Sensitive information includes the identities of communicating parties, network traffic patterns [2]. The leak of such information is often disturbing in security-sensitive situations. For example, an unexpected change of the traffic pattern in a military network may indicate a forthcoming action, a chain of commands, or a state change of network alertness [3]. It may also disclose the locations of command centers or mobile VIP nodes, which will enable the enemies to launch pinpoint attacks on them. In contrast to active attacks, which usually involve the launch of denial of service or other more "visible" and hostile attacks on the target network, traffic analysis is a kind of passive attack, which is "invisible" and difficult to detect. It is therefore important to design countermeasures against such malicious traffic analysis, which leads to the importance of deploying an efficient mechanism that ensure communication anonymity in MANETs.

In this paper, we address two main concerns in MANETs; namely access control and anonymous communication in order to provide a framework for secure communication. Most of the work done only provides separate solutions for each of the two issues, putting into consideration the vitality of the two services as a backbone for secure MANET operations. For real life situations, a

 ISBN: 978-1-61208-503-6

MANET administrator should deploy the two services separately each with its independent cost. In comparison to other monotonic solutions that only provides one service at time, we argue that with a similar or even lower cost the security services can be highly correlated in a single framework that provides MANET nodes with key management, access control and anonymous communication capabilities.

The rest of this paper is organized as the follows. In Section 2, we provide a background for access control and anonymous communication in MANETs and the major proposals that dealt with them. In Section 3, we present the preliminaries that are utilized in developing our proposed solution including elliptical curve with pairing and threshold secret sharing basics. In Section 4, we specify the network model, and the adversary model for the framework design. In Section 5, we present our proposed framework. In Section 6, we provide a performance analysis for our framework in comparison with existing solution.

II. RELATED WORK

Most of the work provided in the literature provides separate solutions for access control and anonymous communication schemes; here we provide a background for each of them.

A. Access Control

Access control for MANETS is a challenging task for a number of reasons [5]:

- First, MANET environment is a distributed problem. It does not have a clear defense line like other types of networks (wired or cellular) which make it difficult to implement the access control mechanism at routers or base stations.
- Second, it's preferable that any access control service will be available at each node locally in order to evade communication over unreliable multihop channels.
- Third, access control solutions should deal with nodes' misbehavior, as network nodes could already hold access control information.
- Finally, as node membership in MANET has a dynamic nature, the solution has to dynamically deal with that.

Kim et al. in [6] presented an early effort to build a framework for network access control using cryptographic techniques and protocols. Their framework classifies admission policy based on the entity which makes the admission decisions (external or internal entity). Despite of, the simplicity and the relative easiness to support these polices, they are inflexible and unsuitable for MANETs.

Zhou and Hass [7] proposed using threshold cryptography [8] to secure MANETs. They suggested distributing CA's (Certificate Authority) public key to each node, while CA's private key distributed among the subset of nodes such that a certain threshold of them can jointly perform certificate generation to the nodes joining the network.

Saxena et al. [9][10] make use of various existing threshold signature schemes to build a distributed admission control mechanisms for ad-hoc groups, but, they did not tackle the problem of group membership revocation.

B. Anonymous communication

Throughout the literature, a number of anonymous communication protocols have been suggested. Most of them come from Chaum's two important approaches: mixnet [11] and DC-net [12]. These protocols discussed three types of anonymous communication properties: sender anonymity, recipient anonymity and relationship anonymity.

- **Sender anonymity:** means that a particular message is not linkable to any sender and no message is linkable to a particular sender.
- **Recipient anonymity:** similarly means a particular message cannot be linked to any recipient and that to a specific recipient, no message is linkable
- **Sender-recipient relationship anonymity (or relationship anonymity in short):** refers to that the sender and the recipient cannot be marked as communicating with each other, though it may be clear they are participating in some communications.

The mixnet family protocols (e.g., [13][14]) make use of special servers that intended to shuffle the received packets to make the communication path (including the sender and the recipient) unclear "ambiguous" these servers called "mix" servers. In order to achieve the desired anonymity, these protocols depend on the statistical features of the underlying traffic which is also called cover traffic. As a result, these protocols are inadequate in dynamic network environments like MANETs where trusted servers are unavailable.

The DC-net family protocols (e.g., [15][16]) use secure multi-party computation techniques. They offer verifiable anonymity without depending on trusted third parties. However, these protocols have transmission collision problem which does not have a concrete solution.

III. PROPOSED FRAMEWORK

The majority of solutions provided to address security of mobile ad-hoc networks only tackle one concern at a time either it be access control, key management, secure routing, anonymous communication, etc. Our proposed framework aims to provide three of the major security services that we believe in its importance in order to provide a concrete and solid secure framework for MANET operations. Our proposed framework provides key management, access

control and anonymous communication and secure in a single coherent framework. We firstly introduced this framework at [17] utilizing the proposed identity based cryptography and access control techniques to provide crucial MANET services, namely address auto-configuration, secure pairwise communication and secure group communication. The main advantage of this framework that it provides the mentioned services without adding an excessive computational or communication overhead compared to existing solution that provides only one of our services. Our proposed anonymous communication scheme is based on an efficient access control mechanism with authenticated key establishment using identity based cryptography and threshold secret sharing techniques.

Our mechanism provides its services without any assumption of a prefixed trust relationship between nodes, which effectively resolves the problem of single point of failure in the traditional public key infrastructure. In this paper, we present an access control mechanism based on the usage of membership access ticket using identity based cryptography primitives. Based on the possession of a valid access ticket, mobile nodes can get involved in a secure communication achieved through our proposed anonymity protocol.

We consider a MANET consisting of *N* nodes, and the network size may change dynamically as nodes may join, leave, or crash at any time. Each node has a unique non-zero ID and assumed to be its MAC address. In order to improve system efficiency in terms of communication and computation, we employed identity-based cryptography (IBC) as an efficient alternative to the traditional public key cryptography techniques to provide essential cryptographic primitives.

Fig. 1 depicts our framework, at the top layer, resides the three main services; access control, anonymous communication which are based on the intermediate layer that provides the key management functionality using IBC primitives provided by the lower layer. Hereafter we describe protocols used to provide our targeted services.
We propose four algorithms that provide collectively the functionality of key management, access control and anonymous communication.

A. Key Management and Access control

Key management functionality in terms of the creation of master public key, master private key share, nodes private key and new master private key share creation for a new node are accomplished through algorithms 1 , 2 and 3. Access control functionality is accomplished based on key management and appears in algorithm 2.

For membership renewal, after the membership access ticket (MAT) of a certain node expires, it sends a request to **K** neighbor nodes, where each of them checks node's behavior, then send signed partial membership token. The requesting node combines partial signature to acquire its new MAT. Nodes behavior observation is out of our scope.

Membership revocation of MAT happens for one or more of the following reasons:

1. Due to expiry of MAT.
2. Due to misbehaving or selfishness.

B. Privacy and Anonymous Communication

It's widely known that privacy is conflict with authentication and certification which achieved only through a trusted third party (TTP) registration but in order to trace any node that would give out false information there must be a registration. Hence when node X transmit a message to node Y, Y needs to check that X is a registered and authenticated node through the certificate that escort the message X, so that any node can be traced if the need arises. The certificate must be signed using certificate authority (CA) private key in order to enable Y to check the validity of the certificate. But in order to protect communicating entities privacy any message sent by one party should appear as if sent by another entity so that pseudonyms are needed, however the pseudonyms should contain some information that let the CA (and only the CA) to determine the true identity of its holder.

Algorithm 1 describes the steps carried out by network nodes in order to cooperatively produce system's master public key based on elliptic curve cryptography (ECC). Based on the concepts proposed by Pedersen [18], we employ ECC to generate the master public key and private key share. In our proposed scheme we operate without any trusted authority support, where the master key pair is computed jointly by the initial network nodes.

Algorithm 1: *Master Public Key and Master Private Key share generation*

1. Each node $\mathbf{n_i}$ randomly chooses a secret $\mathbf{x_i}$ and a polynomial $\boldsymbol{f_i(z)}$ of degree k-1, s.t: fi(0)=xi.
2. Each node ni compute its sub-share for $\mathbf{n_j}$ as SSij= $\boldsymbol{f_i(j)}$, j=1,2,3,...
3. Send SS_{ij} securely to $\mathbf{n_j}$.
4. After receiving **n-1** sub-shares $\mathbf{n_j}$ compute its share of master private key as $S_j=\sum_{i=1}^{k} SS_{ij}$
5. Any coalition of K nodes can recover the secret using $\sum_{i=1}^{k} S_i l_i(z) \bmod q$ where $l_i(z)$ is Lagrange Coefficient.
6. Each shareholder publishes S_iP, where P is a common parameter used by IBS. S_iP is a point multiplication.
7. Master public key $\mathbf{Q_n=\sum_{i=1}^{k} S_i P}$

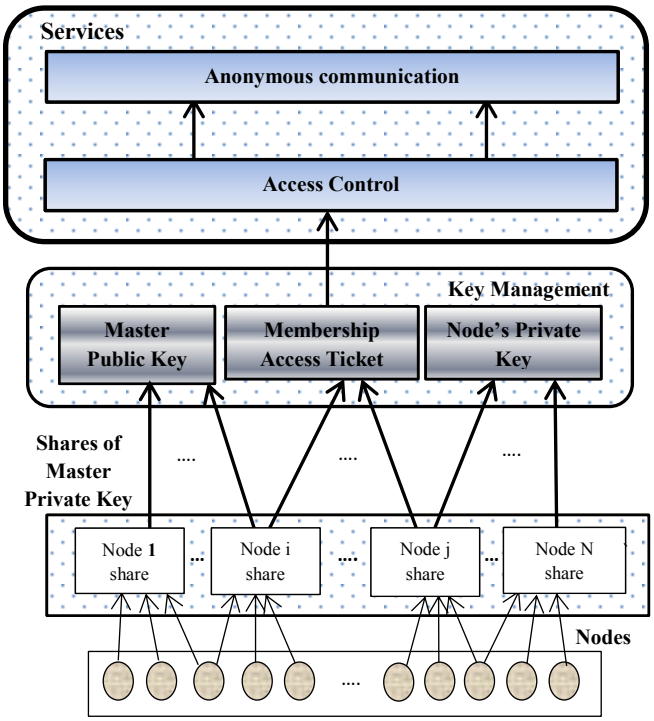

Figure. 1. Proposed Framework.

Algorithm 2 describes the proposed node's private key and access ticket generation process which is the core used to provide access control and anonymous communication services in our frame work. For a node J, in order to get its private key and acquire a ticket that can be assumed as its access key to the network, we assume that, node's J public key (representing node's identity) is the hash value of its MAC address. Then node J should contact at least k of its neighbor nodes presenting its identity (identity-based cryptography) and request private key generation service (PKG) (*if J was unable to find k neighbors locally, node J would move (roam) to another location*). Since all network nodes share the master private key, any node can be a service node.

Each of k nodes generates a share of the new private key SK_{ij} and sends it to node j, which in turn combine all the shares to generate its new private key SK_j. For authentication, as the new node joins the network it presents any required physical proof. And upon authentication by any *t* nodes, each node of them generate a partial membership access ticket MAT_j^i using its share of the master private key S_i on on the public key of the node appended with the expiry time of this ticket Exp_time_j and its issuing time T_j.

Upon reception of partial tickets node J combines then in order to get its access ticket MAT_j. Using MAT_j node J can participate in further network actions and services

.

Algorithm 2: *Private Key and access ticket generation*

1. Node **J** Public key Q_j=H (MAC_ADD).
2. Node **J** Contact at least k nodes and get $SK_{ij}=S_iQ_j$.
3. Node **J** compute its private key as $SK_j= \sum_i^k S_iQ_j$
4. Upon authenticating the new node (maybe using some physical proof) by any **t** nodes of the **k**
   a. Each node **i** Issue a partial membership access ticket (**MAT**):
      $MAT_j^i=\mathcal{S}_i(Q_j||\text{Exp\_time}_j||T_j)$
   b. Node **J** combine partial tickets as $MAT_j=\sum_{i=1}^t S_i\ H(Q_j||\text{Exp\_time}_j||T_j)$

Algorithm 3 describes steps carried out to enable a new node n to get a new share of the master private key, in order to participate in network services. Any coalition of K existing nodes can jointly participate in the process. Each of the participating nodes create a partial share $S_{i,n}$ and send it to the new node which accumulate those shares in order to get its share of Master Private Key.

Algorithm 3: *New Master Private Key share creation for new node n*

1. Each node **i** of **k** generate partial share as $S_{i,n} = S_i\ l_i(n)$, $l_i(n)$ is Lagrange coefficient.
2. Each node **i** send the share to node **n**.
3. Node **n** adds shares to get $S_n=\sum_{i=1}^k S_{i,n}$

So, the true identity of a node should not be known or readable to any other node. A certified authority (or a trusted party) should sign the pseudonym to ensure that it has a trusted signature in order to achieve privacy and authentication. In order to overcome limitations imposed by CA-based architecture, we armed our security framework with an anonymity and privacy features through the usage of the proposed security architecture that utilize identity based cryptography and threshold cryptography in order to the achieve security goals.

Since that our proposed framework's design supports services flow, the privacy and anonymity features are built upon the ability of the node to have a righteous access control through steps accomplished through Algorithm 1 and algorithm 2.

In our proposed anonymity solution, for two parties **Alice** and **Bob** to communicate anonymously they use pseudonyms to conceal their identity as **Carol** and **Dale. Alice** starts with creating an alias identifier rather than its true identity as **Carol,** with this it creates an alias public key ($\mathbf{PK_{als}}$) and its corresponding alias private key ($\mathbf{PrK_{als}}$). Then perform the following steps described in algorithm 4.

 ISBN: 978-1-61208-503-6

Algorithm 4: Privacy and Anonymous Communication

1. Alice generate an alias id (carol) , alias public key (PK_{als}) and alias private key (PrK_{als})
2. Alice sign its MAT with its system generated private key SK_{alice} as its original certificate **Original_Cert =** $SIG_{SK_{alice}}(MAT_{alice})$
3. Alice encrypt Original_Cert combined with its system public key Q_{alice} and a timestamp TS, with system master public key Q_n, producing a system authenticator **Sys_Auth=** E_{Q_n} $(Original\_Cert \parallel Q_{alice} \parallel TS)$, TS change each time to make Sys_Auth looks different each time.
4. Alice send a message **M = (PK_{als}, Sys_Auth,** $SIG_{PrK_{als}}$**(H(entire_message))** to **K** nodes for a partial signature.
5. Each of the **K** nodes, checks signature correctness using PK_{als} and sign the digest of the message (PK_{als}, Sys_Auth) using its share of the master private key S_i and return it to carol (Alice)
   Note: none of the signing nodes can know the identity of the requesting node (Alice), all it do that it sign on the combination **Sys_auth** and PK_{als} and that they belong to the same identity.
6. Alice combine the received partial signatures to make its **Alias_Cert** as the same way a new node gets its private key (algorithm 2).
   Alias_Cert =$\sum_1^k S_i$ **(Life_Span, PK_{als}, Sys_Auth)**
7. To send a message to bob;
   i. Carol (Alice) sign the digest of the message with its alias private key. **Signed_Hash=SIG_{PrK_als}(H(message)||TS)**
   ii. Carol (Alice) send the message as:
   [Alias_Cert || Signed_Hash || message]
8. For privacy, the message can be encrypted with intended recipient public key (bob).

For **Bob** when he receives the message:

1. Use system public key Q_n to verify signature on carol's certificate.
2. If carol's certificate is valid PK_{als} is considered authentic and used to authenticate (verify) signature on carol's signed hash to get **[H(message)||TS]**
3. If message is encrypted using Bob's alias **PK**, he uses his alias private key to decrypt the message.

For Bob to replay as Dale:

1. Do the same steps to get his alias certificate.
2. Send **[Dale's Certificate|| H(carol's message) || Dale's Signed hash || Dale's Message or** $E_{PK_{als}}$ **(Message)]**

In case of the existence of a misbehaving node, our model requires the existence of some arbitrator or some reference entity to manage resolving the issue. If a threshold number of nodes (R) complain about an anonymous node (X), then this node is stripped out of its anonymity to find out its true identity to take the proper actions against. In order to resolve the dispute, a need to reveal the true identity of a misbehaving node (ex. carol) is aroused, and the following steps are carried out:

1. The arbitrator decrypt carol's certificate ($Alias\_Cert$) using system public key Q_n D_{Q_n} ($Alias\_Cert$)= [Life_Span, PK_{als}, Sys_Auth]
   The arbitrator decrypt **Sys_Auth** by sending it to K nodes where each node uses its share of the master private key and the arbitrator combines the responses.
   $\sum_1^k D_{S_i}$ (E_{Q_M} **(Sys_Auth)**) = [$Original\_Cert$ || Q_{alice} || TS]

2. The arbitrator decrypt $Original\_Cert$ using Alice's public key Q_{alice} derived from the decrypted **Sys_Auth** in order to prevent false accusations $D_{Q_{Alice}}(SIG_{SK_{alice}}(MAT_{alice})) = MAT_{alice} = \sum_{i=1}^{t} S_i$ $H(Q_{Alice} \| Exp\_time_{Alice})$

TABLE 1. COMPARISON WITH EXISTING PROTOCOLS

	Sender Anonymity			Recipient Anonymity		Overhead	Latency
	External Nodes	*Internal Nodes*	*Recipient*	*External Nodes*	*Internal Nodes*		
OR	√	√	**NO**	√	√	O(I)	O(I)
BUS	√	√	√	√	√	$O(N^3)$	O(N)
CROWDS	√	√	**NO**	√	**NO**	O(d)	O(I)
KMAT	√	√	√	√	√	$O(N^3)$	O(N)
Proposed	√	√	√	√	√	**$O(N^2)$**	**O(N)**

3. Check $\widehat{e}(Q_n, H(Q_{Alice} \,||\, \text{Exp\_time}_{Alice})) \equiv \widehat{e}(P, MAT_{Alice})$

If the above condition is true, then Alice identity is confirmed, and it is impossible for any other node to use Alice identity for malicious actions.

IV. PERFORMANCE ANALYSIS

As stated earlier existing security solutions for MANET provide security services separately. In our pervious papers [17] we provided a detailed performance analysis for our proposed framework in terms of access control and key management. In this Section, we provide a performance analysis for the integrated protocol for anonymous communication.

A. Comparison with Some Existing Schemes

We provide here a comparison for our proposed protocol with some existing solutions for anonymity in MANET, namely OR[19], Crowds[20], BUS[21], KMAT[22].

Like mixnet-based protocols (OR, Crowds), our proposed solution provides anonymity to the sender and the receiver. Also they do not account on the statistical characteristics of the underlying traffic. Both hide the sender and the receiver from each other. Our proposed solution is more efficient than BUS in terms of overhead as our solution is $O(N^2)$ while BUS is $O(N^3)$, where N is number of the nodes in the network. And unlike BUS our solution permits the receiver to reply without able to identify sender identity and provides broadcasting messages anonymously.

In comparison to KMAT, our proposal achieves the same level of anonymity with a lower communication overhead.

Table 1 shows a comparison in terms of latency and overhead between our proposed solution and the existing ones (where *I* is the number of intermediate nodes, and *N* is the number of the nodes in the network). We can conclude that the proposed solution provides an enhanced anonymity in comparison with current anonymous communication protocols, where with the same or less communication overhead it provides the same anonymity level.

B. Security analysis

Our solution achieved the three types of anonymous communication properties:

- **Sender anonymity**: where none of the transmitted messages can be linked to any sender.
- **Recipient anonymity:** where none of the messages can be linked to a certain recipient
- **Sender-recipient relationship anonymity**: Even it may be clear that two entities are involved in a communication, but they cannot be identified as communicating with each other.

Those three anonymities called full anonymities, as an attacker cannot infer any knowledge about the a sender, a receiver or the communicating parties of any transferred messages from a current traffic

V. CONCLUSION

In this paper, we proposed a secure anonymous communication scheme for MANETs based upon authenticated access control mechanism that ensures the proper behavior within MANET as only nodes with rights to access the network will be involved, which enhances the reliability of the other security functions. The proposed scheme has many advantages over existing solutions as it provides a concrete framework for access control, key management and anonymous communication based on ideas from threshold secret sharing and ID-based cryptography. As results shows the proposed scheme is more efficient than the previously proposed solution for anonymity in addition to the extended capabilities of the proposed framework which also support access control and key management services which can be further extended to provide more security service for MNAETs. Due to the usage of threshold and identity based cryptography our proposed framework exhibits an optimized performance feature. Throughout this work we showed how we can enforce access control through making it a mandatory component in order to get access to other services like anonymous communication. The deliverables from the access control stage is used as a key in the subsequent stage in a way that make smooth service integration. Measurement results and performance analysis indicate that our solution provides an integrated framework for secure communication with an overall performance that outcome existing solutions, which make it more suitable in MANET environment.

REFERENCES

[1] L. Haiyun, K. Jiejun , P. Zerfos and L. Songwu, "URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks", Networking, IEEE/ACM Transactions on (Volume:12, Issue: 6), pp.1049-1063, 2004.

[2] Lou and Y. Fang, "A Survey on Wireless Security in Mobile Ad Hoc Networks: challenges and available solutions", Book chapter in Ad Hoc Wireless Networking, Kluwer, pp. 279–294, 2009.

[3] Y. Kim, D. Mazzocchi, and G. Tsudik, "Admission Control in Peer Groups," IEEE International Symposium on Network Computing and Applications (NCA), pp. 104-113, 2003.

[4] DARPA. Research Challenges in High Confidence Networking. July 1998.

 ISBN: 978-1-61208-503-6

[5] B. Qing-hai , Tongliao, “Comparative research on two kinds of certification systems of the public key infrastructure (PKI) and the identity based encryption (IBE)”, Cross Strait Quad-Regional Radio Science and Wireless Technology Conference (CSQRWC), pp. 147 – 150, 2012.
[6] L. Zhou and Z.J. Haas, “Securing ad hoc networks”. IEEE Network, vol. 13, Issue 6, pp. 24–30, 1999.
[7] Shamir, “How to share a secret”. Communications of the ACM, volume 22, issue 11, pp. 612–613, 1979.
[8] N. Saxena, G. Tsudik, and J. H. Yi, “Access Control in Ad Hoc Groups” International Workshop on Hot Topics in Peer-to-Peer Systems (HOT-P2P), pp. 2 – 7, 2004.
[9] N. Saxena, G. Tsudik, and J. H. Yi, “Threshold Cryptography in P2P and MANETs: The Case of Access Control,” International Journal of Computer and Telecommunications Networking, vol. 51, issue 12, pp. 3632-3649, 2007.
[10] D. Chaum, “Untraceable Electrical Mail, Retrun Address, and Digital Pseudonyms”. Communications of the ACM, volume 24, issue 2, pp. 84–88, 1981.
[11] D. Chaum, “The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability”. Journal of Cryptology, volume 1, pp. 65–75, 1988.
[12] C. Huseyin, “Anonymous Communications in Mobile Ad Hoc Networks”, Phd-Kongens Lyngby, 2006.
[13] M. Reiter and A. Rubin, “Crowds: Anonymity for Web Transaction”. ACM Transactions on Information and System Security, volume 1, issue 1, pp. 66–92, 2000.
[14] L. Ahn, A. Bortz, and N. Hopper, “K-anonymous message transmission”. In Proceedings of the 10th ACM conference on Computer and Communications Security, Washington D.C., USA, pp. 122–130,2003.
[15] P. Golle and A. Juels, “Parallel Mixing”. In Proceedings of the 11th ACM Conference on Computer and Communications Security, Washingto D.C, USA, pp. 220-226, 2004.
[16] Ehab E. Zakaria., H. S. Hamza, and I. A. Saroit, "An Integrated Security Framework for Access Control and Address Auto-configuration for MANETS", WMNC 2015, 8th IFIP Wireless and Mobile Networking Conference, Minich, Germany, pp. 253 – 260, 2015.
[17] T. P. Pedersen, “A Threshold Cryptosystem Without A Trusted Party,” EUROCRYPT, pp. 522-526, 1991.
[18] P. F. Syverson, D. M. Goldschlag, and M. G. Reed, “Anonymous connections and onion routing”. In Proceedings of IEEE Symposium on Security and Privacy, Oakland, CA, pp. 44–54, 1997.
[19] M. Reiter and A. Rubin. “Crowds: Anonymity for Web Transaction”. ACM Transactions on Information and System Security, volume 1, issue 1, pp. 66–92, 1998.
[20] A. Beimel and S. Dolev, “Buses for Anonymous Message Delivery”. Journal of Cryptology, volume 16, pp 25–39, 2003.
[21] L. Ahn, A. Bortz, and N. Hopper, “K-anonymous message transmission”. In Proceedings of the 10th ACM conference on Computer and Communications Security, Washington D.C., USA, pp. 122–130, 2003.

 ISBN: 978-1-61208-503-6