An Outlook on Cryptographic and Trust Methodologies for Clusters Based Security in Mobile Ad Hoc Networks

V. S. Janani and M. S. K. Manikandan
Department of Electronics & Communication Engineering, Thiagarajar College of Engineering
GST Road, Thiruparankundram, Madurai, Tamil Nadu 625015, India
jananivs@tce.edu

(Received Nov. 24, 2016; revised and accepted Mar. 31, 2017)

Abstract

Most of the researches in Mobile Ad Hoc Networks (MANETs) are closely related to security aspects and security issues. However, providing a security mechanism implicitly has been a major challenge in such ad hoc environment due to the dynamic movement of nodes. There are many security protocols as well as key management methods designed in a Public Key Infrastructure (PKI) to handle these MANET issues. To obtain a better understanding of various cryptographic and trust based security aspects, that forms an integral part of the solutions for issues in a clustered MANET, we provided a study on such security features. Through this study, security aspects such security attacks, security services, security challenges, and security solutions are described in a detailed manner.

Keywords: Clustering; Cryptography; MANET; PKI; Trust

1 Introduction

In traditional wireless networks, the existence of infrastructure enables secure communications between nodes on the network, over a limited geographical area [15]. Now-a-days, the demand for faster network setup without any access point or infrastructure is getting increased. Mobile Ad hoc Network (MANET) has been introduced as a solution for such requisites to provide communication over various applications [8]. MANET [14, 29] is defined an infrastructure less IP based cluster of mobile node or computing device, interrelated through multi-hop wireless links.

In MANET, the nodes possess a non-centralized administration system and so the nodes can join or leave freely, to obtain dynamic network topology. Every node in a MANET links to the nearby nodes over transmission range and may work as a router as well as host simultaneously. To communicate with a node, the source node forwards the data to the destination node through its neighboring nodes. Similar to the wired network, the neighbor node in MANET will perform as a router, which makes it a challenging task to detect malicious/legitimate nodes among the neighboring nodes.

Even though trust among the nodes is considered to perform co-operative communication within the network, MANET has more security threat while comparing with infrastructure-based wireless networks. Also, the dynamic environment, inadequate resources (*i.e.* battery power, bandwidth, storage, *etc.*), and lack of centralized monitoring make all communication layers in MANET vulnerable to various attacks. Therefore, MANETs must offer guaranteed for several security levels in order to have effective deployment and usage.

A MANET consists of mobile nodes with an autonomous system that may have gateway to an interface or function in isolation. The topology of the network may vary with respect to the continual node movement and the changes in transmission/reception parameters such as coverage patterns, power levels and interference levels of co-channel. Wherefore, MANETs have several salient characteristics [10, 16] as follows, which make MANETs more vulnerable than conventional networks.

- Infrastructure-less: The absence of static routers, centralized server, and other hardware infrastructures prevents the positioning of central host relationships. A distributed cooperative system is maintained in MANET to cope up with centralized functionalities.

- Wireless link usage: An adversary in wired network must passes through many defence lines at gateways and firewalls. Whereas, attacks on MANET can arise from various sources targeting any node in the network. Every node must be organized to secure against threats as a MANET does not have a clear defence line.

- Multi-hop: Hosts can act themselves as routers due

to the absence of centralized routers and gateways. Therefore, the packets follow multi-hop routes and move across distinct mobile nodes before receiving at their ultimate destination. Multi-hop feature presents a severe vulnerability because of the possible undependability of such mobile nodes.

- Node movement autonomy: Mobile nodes can be freely traversed in the network as they are usually autonomous units. This clearly shows that following down a specified mobile node in large-scale MANET cannot be completed easily.
- Amorphous: The nodes can join and leave the network unexpectedly due to dynamic node mobility and wireless connectivity. This leads topology changes with accidental link formation and breakage. This feature must take into account at any security solution.
- Memory and power limitation: The hosts in MANET are lightweight and have inadequate storage. These shortcomings make the network liable to energy starvation attack or sleep deprivation torture attack, where the attackers may aim some batteries of nodes to detach them. While designing the solutions towards security for MANETs, these features are also considered as a challenging constraint.

In this paper, we seek to provide a review on various methodologies for providing security in a cluster based MANET. We consider cryptography and trust as the two major dynamics that help in security establishment especially for cluster based ad hoc nodes.

2 Security Aspects in MANET

This section designates security aspects in MANET, which includes security attacks, security services and security challenges [9, 10, 17, 19, 20, 27].

2.1 Security Attacks on MANET

The MANET consists of miscellaneous nodes which may includes a malicious/ attacker node that affects the functionality of different MANET layers.

The Table 1 lists out the attacks at various MANET layers. The attacks mainly fall under two main classes: active attack or passive attack. The characteristics of MANET are vulnerable to the below mentioned attacks [5].

Active attacks: This type of attack tries to modify the protocol behavior by performing the operations like replication, modification, and deletion of interchanged data. It destroys or prevents message flow between the nodes. This can be collectively termed as Denial-of-Service (DOS) attacks, which completely block and damage the communication among the nodes.

Table 1: MANET attacks

MANET layers	Type of Attacks
Physical layer	Eavesdropping Jamming Active Interference
Link layer	Selfish node misbehavior DOS Attack Resource Exhaustion
Network layer	Black Hole Attack
	Wormhole Attack Routing Table Poisoning Attack Sleep Deprivation Attack Impersonation Attack Node Isolation Attack Location Disclosure Attack Rushing Attack Blackmail Attack The Invisible Node Attack (INA)
Transport layer	Session Hijacking
Application layer	Malicious code attacks
Multilayer attacks	Denial of Service Impersonation attacks Man-in-the-middle attacks

Passive attacks: This attack includes unauthorized snooping of information, packet eavesdropping and sometimes disabling a prime node from communication. This brings down the network and it contains: hidden channels, traffic analysis and unstable compromised keys.

2.2 Security Services on MANET

The most important security services that safeguard MANET resources from attacks are described as follows [30]:

- Authentication: It guarantees that a node is the one that has to be. Using this mechanism, only authorized nodes can communicate or transmit the data.
- Availability: This security service is employed to preserve the network resources obtainable to legitimate users. It also assures a reliable and appropriate use of data or the network.
- Data Confidentiality: The goal of this security service is to kept information confidential from disclosure [4] and it must be obtainable only to the intended party. This can be implemented via many data encryption methods.
- Data Integrity: The integrity of the data guarantees transmitted or communicated data is not being changed by any other mischievous node.

- Non-repudiation: In non-repudiation service, both sender and receiver would not be able to repudiate a transmitted message.
- Resilience to attacks: Even though a node is compromised partially, this security service makes it tolerant the functionalities of the network.

2.3 Security Challenges on MANET

Many complicated security challenges [11,13,21,23,28,33] that occurred in a MANET are addressed as follows:

- Dynamic Topology: In a MANET, establishing trust between the nodes is very complex as node may join or leave dynamically and changes frequently.
- Lack of Central Authority: Implementing security without any infrastructure or central authority in the network is a challenging job in a MANET.
- Insecure Environment: In a MANET, malicious node can attack and bargain the data while the nodes are moving randomly.
- Routing: In a MANET, routing protocols are most significant, where the nodes mobility varies very often. These protocols are employed for identifying the optimal path from source to destination node. Also, they are developed to exchange the information about routing [21].
- Multicasting: Traditional protocols of wireless networks do not suit one-to-many communication process named multicasting due to MANET characteristics [28,31]. An efficient protocol is required to meet various multicasting challenges.
- Energy Constraints: Mobile nodes will run with battery power, as to manage and avoid node termination. Energy management plays a vital role in MANET due to divers MANET challenges.
- Quality of Service (QoS): The major objective of the QoS is to offer better network services by accurately utilizing the resources of a network. Depending upon the user and application, QoS gathers bandwidth, delay, loss, etc to satisfy their tasks.
- Security: MANET is extremely susceptible to several security attacks, because of its existing key characteristics. It is very hard to accomplish security goals, where the intruders can easily damage the network. While manipulating security solutions, the distinctive features of MANET must be considered with higher priority.
- Clustering: In a MANET, the nodes are separated into virtual groups called clusters, to accomplish scalability even in the existence of high mobility in the network.

3 Security Mechanisms in MANETs

3.1 Cryptography

Generally, cryptography is considered as a powerful tool [6] introduced to construct and analyse various security protocols, by providing all the required network services. However, it can also be defined as a process by which plain text (original data) can be converted into cipher text (scrambled data) and vice versa, using secret keys. It can be classified into two types depending on the secret key used: *Symmetric/private key cryptography* (where the message is encrypted and decrypted with a single key) and *Asymmetric/public key infrastructure (PKI)* (where the information is processed by two different keys). Nevertheless, all these cryptographic techniques are the primitives of security, which can be widely utilized in both wired and wireless networks to provide confidentiality, authentication, integrity, and non-repudiation [4].

Most of the researches in MANET rely on the fact that there exist cryptographic mechanisms to secure keys, for various applications. Many researchers have suggested asymmetric cryptographic techniques to handle ad hoc protocols. But the infrastructure-less MANET makes it a challenging task especially during asymmetric signature verification. To get the better of the challenge, symmetric key techniques were proposed.

3.2 Public Key Management

To deploy PKI system in MANETs two main alternatives have been suggested as: distributed or non-centralized Certification Management, and self-organized PKI management. In distributed certificate management, the certification processes are supported by distributed Certificate Authorities (CA) that issue and validate certificates for each node.

Self- Organized key management have become a principal solution for any secure communication that incorporates the procedures and techniques to support the cryptographic keying relationships among certified parties. Besides, it establishes many services such as key initialization, key generation, key distribution, and key updating of the network. In key management, a key can be established [26] either using key agreement or key distribution protocols.

The key agreement protocols are characterized by the absence of trusted authorities responsible for key management, in which a key is constructed by two or more node collaboration. While, in a key distribution protocol a single node generates and distributes keys to other nodes in the presence of trusted authorities. The distribution protocol can be categorized into symmetric or asymmetric (certificate based, identity based) schemes, to make it suitable for ad hoc nature. Although key agreement schemes have not designed certainly for MANET, it fits the wireless environment. There are numerous key

Table 2: Key management methods in MANET

Schemes	Types
Symmetric Key Management	Distributed KeyPre Distribution Scheme Peer Intermediaries for Key Establishment Key Infection
Asymmetric Key Management	Self-Organized Key Management Secure and Efficient Key Management Private ID Based Scheme
Group Key Management (GKM)	Centralized Distributed Decentralized Simple and Efficient GKM Private Group Signature Key
Hybrid Key Management	Cluster Based Composite Scheme Zone-based scheme

management methods employed to accomplish greater security using cryptographic keys. Some of those key management methods in MANET are mentioned below in Table 2.

Moreover, the certificate based key distribution requires digital certificates signed by a trusted CA to bind public keys to authenticated nodes. These certificates encompass key materials, owner nodes identity and valid digital signatures, to make trust on the signer. In contrast with certificate based PKI scheme, identity based scheme uses nodes identity signed by a trusted entity as public key.

Most of the solutions introduced to cryptography were intended to secure data forwarding and routing mechanisms [6]. Moreover, due to the lack of any central administration in MANETs, key management has been a challenging issue. Certainly, this infrastructural role should be distributed among all nodes to form a key based infrastructure. Hence, the key management scheme of MANETs does not trust or rely on any stable CA, but indeed it should be self-organized and distributed.

4 Trust Models

Trust is one of important security characteristic that enables nodes to cope with the uncertain nature of MANET and consequently, trust calculation as well as management is difficult in MANET [2,7,24,34]. An untrustworthy node certainly has adverse affects the performance of the network. Therefore, calculating the trust level of each node has a promising influence on the security with which a node can be a part of a secure communication.

4.1 Trust Calculation Model

The trust calculation can be broadly classified into two types: Centralized and Decentralized trust models.

1) Centralized trust model:
Most of the centralized trust models assume one or more Trusted Third Party (TTP) as a central entity to compute and manage trust [7]. It is trusted by all nodes and is frequently employed for providing key management services. The TTP either calculates the trust for entire MANET or provides the initial trust value to each node. The centralized trust can be calculated by different methods:

Cluster based trust model: Trust is calculated by combining the initial trust obtained from the header node with the individual trust. This individual trust value may be based on the successful/unsuccessful experiences with the neighboring nodes during data communication.

Representative based trust model: Reputed representatives/agents are deployed by each node to assist the trust calculation in this model. To compute trust of neighboring nodes, each node verifies about those neighbors with their representatives. Final trust is calculated with the obtained trust value from the agent with the individual value.

Leader based trust model: A distributed trust is maintained at each group, where the group leader calculates the final trust based on the direct observations and the collective trust obtained from the group members.

2) Decentralized trust model:
Due to the lack of maintaining a global trusted entity in MANET, each node computes trust on its neighbors by itself, in decentralized model. Here the trust can be calculated by using any of the following three methods.

Direct trust: Each node observes the communication of its neighboring nodes and keeps a record of those communications within it. To compute trust, the trustor node weighs its own record with the record received from the trustee and other neighboring nodes. Direct trust can be computed by different ways as: packet routing and past-present observation methods.

Indirect trust: Decentralized trust can be calculated indirectly based on the recommendation of the neighboring nodes on a target node. This can be achieved either by voting method or by flooding the recommendation throughout the MANET.

Hybrid trust: This model takes advantage of the optimistic features of both direct and indirect trust models. It integrates direct observations and recommendations to compute trust effectively.

The absence of stable trust entities, resource limitations, frequent link failures and other security vulnerabilities makes the decentralized trust models a challenging one. To manage these issues, most of the methods proposed so far assumed to have a centralized trust entity.

4.2 Trust Application in MANET

From decades, cryptography has been considered as the most prominent methodology to secure the network from adversaries. It comprises of only an initial security check in terms of authentication, confidentiality, integrity and non-repudiation. Those methodologies, in fact provided only a partial solution from which an attacker node can easily impersonate. The threats that alter the credential security (soft security threats) cannot be eliminated completely with these methods. Trust has been widely applied in MANET not as a replacing methodology [12], but as an accessory to work against the opponents. Trust mechanisms and cryptography can be deployed together to provide a complete solution to the security threats in MANET [18].

5 Clustering Methodology

Clustering can generally be defined as the grouping of nodes in a network into an interrelated sub-structure [3]. In a MANET, a clustering scheme partitions the mobile nodes into virtual groups called clusters [1, 3, 32]. There are three main components in a cluster-based network: Cluster Head (CH), Cluster Members (CM) and Cluster Gateway [25]. Figure 1 shows typical cluster architecture in a mobile ad hoc network. The CH assists as a leader for its group, carrying out different cluster activities as packet forwarding, inter-intra communications clustering and so on. The CMs are ordinary nodes which reside in various clusters. A cluster gateway is nothing but an intermediate non- CH node that connects two adjacent clusters. The survey on clustering schemes evidently shows its achievement in MANET performance, especially in maintaining the topology. Some of the benefits of clustering in MANET are:

- Maximize the capacity of network by reusing existing resources. Similar set of frequency is employed only when two clusters are not adjacent and overlapped.
- Among adjacent clusters, CH and border nodes generate a virtual backbone for a beneficial routing.
- Minimize the storing information overhead by updating only the information of mobile nodes that relocated to another cluster.
- Decrease of control packet.
- Stability, simplification, and localization.

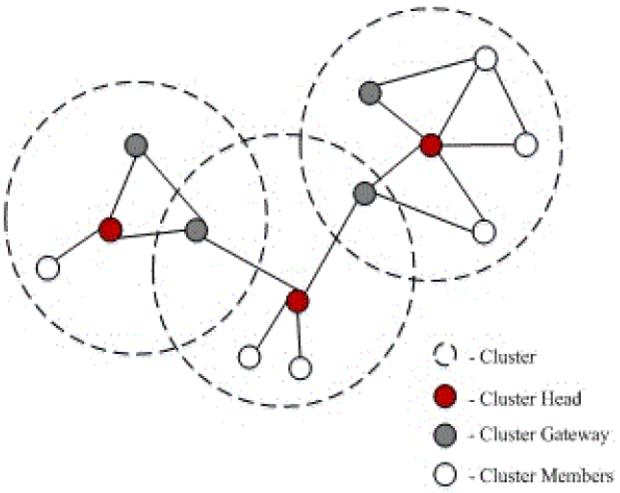

Figure 1: Cluster architecture in a MANET

5.1 Clustering Approaches in MANET

Clustering in MANET is performed based on different criteria as given below:

Minimized Dominating Set based clustering: This clustering approach is used to discover a minimum/weakly connected dominating set for a given network. It decreases the number of nodes that contributes in route search or maintenance of routing table and constructs CHs to proceed inter- cluster communication rapidly. *Example:* Connected Dominating Set (CDS) and weak CDS based clustering methods.

Low cost maintenance clustering: In order to minimize the clustering-based maintenance cost, a cluster infrastructure is provided for upper layer applications. *Example:* Least Cluster Change (LCC), Passive Clustering (PC), and 3-hop Between Adjacent Cluster head (3hBAC).

Mobility-aware clustering: Here, the mobility characteristic of the MANET nodes is considered for cluster construction and maintenance. This approach assigns the mobile nodes with low relative speed within a cluster to maintain the connection. *Example:* Mobility Based Metric for Clustering (MOBIC) and Distributed Dynamic Clustering Algorithm (DDCA).

Energy-efficient clustering: In order to proliferate the network lifetime, this approach either avoids or balance unnecessary energy consumption of mobile nodes. *Example:* Energy based Dominating Set and Identity based Load Balancing Clustering (IDLBC).

Power- aware clustering: To save the battery power in MANET, power aware clustering can be done by load-balancing, reducing the size of dominating set or by minimizing the consumption of transmission

energy. *Example:* Degree-Load-Balancing Clustering (DLBC).

Other-metrics-based clustering: Clustering can also be performed based on various metrics such as identity of nodes, size of cluster, degree of node, weight of cluster *etc.* *Example:* Weighted Clustering Algorithm (WCA), and On-Demand WCA.

5.2 Clustering Schemes from Security Perspective

A clustering scheme can be secured with various mechanisms as (1) cryptographic-based clustering (2) trust-based clustering and (3) hybrid clustering methods.

1) Cryptographic-based Clustering Methods:
The security of clustering operation against attackers has been increased with traditional cryptographic-based clustering methods. But, the insider attackers and compromised nodes remain undetected. This can be protected by using trust and reputation management methods. In MANETs, these methods have high overheads and inadequate resources. Therefore, secure clustering methods predominantly focus on defending the current CHs and choosing valid and accurate node as novel CH. Moreover, several security attacks can be accompanied against clustering. Following is the classification of attacks on clustering schemes [22] as

   - Clustering operation attacks;
   - Cluster maintenance; operation attacks;
   - Cluster component attacks.

   Cryptographic-based clustering methods employ cryptography for protecting networks against security threats. This offers security services like data privacy, digital signatures, and authentication. Depending on the key management techniques, the cryptographic security solutions are set to be high.

2) Trust-based Clustering Methods:
Trust-based clustering methods incorporate the trust management methods along with the clustering techniques. This can decrease the reputation management overheads. For each node, these methods accomplish the trust-based information. It further avoids the election of misbehaving nodes as cluster components. There are mainly two kinds of trust-based clustering method: pure and hybrid.

   Pure trust based clustering: This method comprises two main purposes: (1) enhancing the security of network by selecting reliable nodes as CHs, (2) minimize the trust management system overheads. This method is liable to numerous attacks like self-promoting attacks and bad mouthing. These security systems do not for entire protection against attackers and are susceptible to mischievous nodes and internal malicious nodes.

   Hybrid trust based clustering: These methods are the most difficult security solutions, which incorporate the cryptography-based techniques and reputation management schemes with clustering methods. This can protect against both internal and external attackers as it creates complex and strong solutions towards security. It also has the highest level of resource consumption.

6 Conclusion

This paper provides a brief introduction to the MANET and its key characteristics. In the subsequent section, the security aspects such as attacks, security services and security challenges are described in a detailed manner. The core domain of this research which comprises the security mechanisms, trust model and clustering approaches are explained with their appropriate examples in the following sections. The security mechanisms cover an overview of two predominant tools of wireless networks; cryptography and public key management.

References

[1] M. Alinci, E. Spaho, A. Lala, V. Kolici, "Clustering algorithms in MANETs: A review," in *IEEE Ninth International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS'15)*, DOI: 10.1109/CISIS.2015.47, 2015.

[2] A. Ankit, A. K. Verma, "A review & impact of trust schemes in MANET," in *Proceedings of the International Conference on Advances in Information Communication Technology & Computing (AICTC '16)*, 2016.

[3] A. Bentaleb, A. Boubetra, S. Harous, "Survey of clustering schemes in mobile ad hoc networks," *Communications and Network*, vol. 5, no. 2, pp. 32-48, 2013.

[4] B. S. Bhawani, V. Pallapa, "Performance analysis of location privacy preserving scheme for MANETs," *International Journal of Network Security*, vol. 18, no. 4, pp. 736-749, 2016.

[5] W. Bing, J. Chen, J. Wu, M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc networks," in *Wireless Network Security, Signals and Communication Technology*, pp. 103-135, 2007.

[6] W. Bing, J. Wu, M. Cardei, "A survey of key management in mobile ad hoc networks," in *Handbook of Research on Wireless Security*, vol. 8, no.3, pp. 48-66, 2007.

[7] J. H. Cho, C. I. Ray, K. S. Chan, "Trust threshold based public key management in mobile ad hoc networks," *Ad Hoc Networks*, vol. 44, pp. 58-75, 2016.

[8] M. Conti, C. Boldrini, S. S. Kanhere, E. Mingozzi, E. Pagani, P. M. Ruiz, M. Younis, "From MANET to people-centric networking: Milestones and open research challenges," *Computer Communications*, pp. 1-21, 2015.

[9] P. Di, S. Guarino, N. V. Verde, J. D. Ferrer, "Security in wireless ad-hoc networks: A survey," *Computer Communications*, vol. 51, pp. 1-20, 2014.

[10] D. Djenouri , L. Khelladi, N. BadXache, "A survey of security issues in mobile ad hoc networks," *IEEE Communications Surveys*, vol. 7, no. 4, pp. 2-28, 2005.

[11] A. Dorri, R. K. Seyed, K. Esmaeil, "Security challenges in mobile ad hoc networks: A survey," *International Journal of Computer Science & Engineering Survey (IJCSES'15)*, vol.6, no.1, pp. 15-29, 2015.

[12] P. Gera, G. Kumkum, G. M. Manoj, "Trust-based multi-path routing for enhancing data security in MANETs," *International Journal of Network Security*, vol. 16, no. 2, pp. 102-111, 2014.

[13] P. Godwin, D. R. Srinivasan, "A survey on MANET security challenges, attacks and its countermeasures," *International Journal of Emerging Trends & Technology in Computer Science*, vol. 3, no. 1, pp. 274-279, 2014.

[14] C. J. Hee, A. Swami, R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 4, pp. 562-583, 2011.

[15] A. Hinds, M. Ngulube, S. Zhu, A. A. Hussain, "A review of routing protocols for mobile Ad-Hoc networks," *International Journal of Information and Education Technology*, vol. 3, no. 1, pp. 1-5, 2013.

[16] C. Jianmin, J. Wu, "A survey on cryptography applied to secure mobile ad hoc networks and wireless sensor networks," *Handbook of Research on Developments and Trends in Wireless Sensor Networks: From Principle to Practice*, pp. 262-289, 2010.

[17] A. Kartit, K. I. Hamza, B. Mohamed, "Improved methods and principles for designing and analyzing security protocols," *International Journal of Network Security*, vol.18, no.3, pp. 523-528, 2016.

[18] A. Kumar, G. Krishna , A. Alok, "Design and analysis of lightweight trust mechanism for secret data using lightweight cryptographic primitives in MANETs," *International Journal of Network Security*, vol. 18, no. 1, pp. 1-18, 2016.

[19] C. T. Li, M. S. Hwang, "A lightweight anonymous routing protocol without public key en/decryptions for wireless ad hoc networks",*Information Sciences*, vol. 181, no. 23, pp. 5333–5347, Dec. 2011.

[20] C. T. Li, M. S. Hwang, C. Y. Liu, "An electronic voting protocol with deniable authentication for mobile Ad hoc networks," *Computer Communications*, vol. 31, no. 10, pp. 2534–2540, June 2008.

[21] C. Mahima, M. Ahmad, M. Waseem, "Review on MANET: Characteristics, challenges, imperatives and routing protocols," *International Journal of Computer Science and Mobile Computing*, vol. 3, no. 2, pp. 432-437, 2014.

[22] M. Maleknasab, M. Bidaki, A. Harounabadi, "Trust-based clustering in mobile ad hoc networks: Challenges and issues," *International Journal of Security and Its Applications*, vol. 7, no. 5, pp. 321-342, 2013.

[23] K. Mohit, R. Mishra, "An overview of MANET: History, challenges and applications," *Indian Journal of Computer Science and Engineering*, vol. 3, no. 1, pp. 121-125, 2012.

[24] Z. Movahedi, H. Zahra, B. Fahimeh, P. Guy, "Trust-distortion resistant trust management frameworks on mobile ad hoc networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1287-1309, 2016.

[25] M. U. Muhammad, M. Amjad, S. Houbing, "SeCRoP: Secure cluster head centered multi-hop routing protocol for mobile ad hoc networks," *Security and Communication Networks-Wiley*, vol. 9, no. 16, pp. 3378-3387, 2016.

[26] K. Pratibha, N. Goyal, "Survey of various keys management techniques in MANET," *International Journal of Emerging Research in Management &Technology*, vol. 4, no. 6, pp. 176-178, 2015.

[27] K. Praveen, P. C. Sekhar, N. Papanna, N. B. B. Bhushan, "A survey on MANET security challenges and routing protocols," *International Journal of Computer Technology and Applications*, vol. 4, no. 2, pp. 248-256, 2013.

[28] G. Priyanka, V. Parmar, R. Rishi, "Manet: Vulnerabilities, challenges, attacks, application," *International Journal of Computational Engineering & Management (IJCEM'11)*, vol. 11, pp. 32-37, 2011.

[29] A. Rana, D. Sharma, "Mobile ad-hoc clustering using inclusive particle swarm optimization algorithm," *International Journal of Electronics and Information Engineering*, vol. 8, no. 1, pp. 1-8, 2018.

[30] S. Sen, J. A. Clark, J. E. Tapiador, "Security threats in mobile Ad hoc networks," in *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET, Al-Sakib Khan Pathan, Ed. Boca Raton, Florida: Taylor & Francis*, 2010.

[31] M. Stanek, "A note on security protocol for multicast communications," *International Journal of Network Security*, vol. 14, no. 1, pp. 59-60, 2012.

[32] S. Victor, R. Ayman, H. Marques, J. Rodriguez, S. Vahid, R. Tafazolli, "A survey on clustering techniques for cooperative wireless networks," *Ad Hoc Networks-Springer*, vol. 47, pp. 53-81, 2016.

[33] V. K. Vishakha, N. K. Bhil, "Mobile ad-hoc network (MANET) and its security aspects," *International Journal of Advance Research in Computer Science and Management Studies*, vol. 3, no. 8, pp. 145-149, 2015.

[34] G. Xu, Y. Zheng, "A survey on trust evaluation in mobile ad hoc networks," in *Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications*, pp. 140-148, 2016.

Biography

V. S. Janani received her B.E. degree in Electronics and Communications Engineering from Anna University in 2009 and M.E degree in Embedded System Technologies from Anna University in 2011.Since 2012 she has been pursuing her PhD degree in the department of Electronics and Communication Engineering at Thiagarajar College of Engineering.

M. S. K. Manikandan received his B.E. degree in Electronics and Communications Engineering from National Institute of Technology. Trichy, Bharathidasan University in 1998 and M.E degree in Communication System from Madurai Kamaraj University in 2000. He received his PhD in Wireless Communication from Anna University; Chennai in 2010.He has been working as associate professor in Thiagarajar college of Engineering for years. He has been serving as reviewer for several IEEE conferences, Springer, IET and other international journals.