Survey of Cryptography Techniques against Impersonation Attacks in MANET

P. Kavitha
Research Scholar
Hindustan University
Padur, Chennai

Rajewsari Mukesh, PhD
Professor
Hindustan University
Padur, Chennai

ABSTRACT
Security is the main concern in Mobile Ad Hoc Networks (MANETs). There are numerous malicious activities performed on single as well as multi-layer of the MANET. Unlike specific layer attacks, the multi-layer attacks are intelligent, since they can coordinate the misbehaving activities in various layers and launch further sophisticated attacks. Most of the research works have focused only on the specific layer attacks. However, there is little progress in providing secure communication against multi-layer attacks. The security against impersonation attack is difficult and to provide the multi-layer protection becomes crucial. To meet the security requirements, several security algorithms have been proposed. However, solutions to the impersonation attack are still incomplete. The routing behavior analysis is insufficient to provide multi-layer protection against impersonation attack, and thus the cryptographic mechanism is widely used for providing authentication and preventing impersonation in MANET. This work conducts a survey on network attacks and conventional security solutions with its advantages and limitations. Finally, this work explores the complexities of symmetric, asymmetric, and group key management.

Keywords
Wireless networks, secure communication protocol, Cryptography, Key management, and Impersonation

1. INTRODUCTION
Wireless Mobile Adhoc Networks (MANETs) are popular and receives a great deal of attention in wireless communication, due to its easy deployment with low cost. The MANETs form a self-organized network in a shared wireless medium without the aid of permanent infrastructure. The shared wireless medium as well as lack of design to monitor the traffic and accessibility lead to the security threats at all layers of MANET [1]. The defense mechanism against network attacks has to consider the most important design goals like availability, reliability, resiliency, and self-healing. The availability defines the possibility of service access that ensures the data delivery at any time even in the face of attacks. The interrelated factors to the service availability are resilience and self-healing. The term resilience denotes the attack tolerance and the ability of the network to continuously offer uninterrupted services to the users. The self-healing is the ability of recovering the network from security threats. The multi-layer attack can coordinate the misbehaving activities in various layers to achieve their goal. This leads the multi-layer attack to launch further sophisticated attacks. For example, the impersonation attack captures the physical node and compromises its secrets, such as cryptographic keys [6]. After compromisation, the attackers can spread malicious data, drop the data, modify the data, and know others secret data easily. Moreover, the impersonation attacks reduce the probability of attacker detection due to the compromisation. Several defense mechanisms have been proposed for impersonation attack at different layers. The defense techniques can be categorized into proactive and reactive. The proactive defense techniques are deployed before the attacks are launched in the network, whereas the reactive defense techniques come into action during an attack. The example of proactive defense techniques is as follows: In MANET, the purpose of the confidentiality and integrity is to initialize and deliver the data in a secure manner using cryptosystem. The secure cryptosystem provides a unique identity to each user and verifies the credentials of the users during communication [3]. This is then maintained by the secure key management. Using the keys, the nodes encrypt the transmitted data and ensure the data confidentiality. The example of reactive defense mechanisms is an Intrusion Detection System (IDS) and trust. It can identify the attacks that can pass through the proactive defense mechanism.An IDS in MANET is independent of the network specifications, and it is designed without involving it in the routing activities of a node [4]. The data delivery reliability assurance is provided in network layer using trust measurement. The concept of trust defines the belief level of a node based on the routing behavior [5].

2. LITERATURE REVIEW
Security is a main issue that needs to be considered in wireless communication. The MANET is vulnerable to different attacks, due to the wireless medium and adhoc nature. The network attacks are classified into active and passive attacks and both of them can be launched in various layers as shown in figure: 1. The active attacks are further classified into internal and external. The compromised nodes internally initiate attacks in the network, named as internal attack, whereas in external attack, the nodes that do not belong to the network attack the communication [2]. The detection of internal attacks is more complex than the external attacks.

In physical layer, the MANET is vulnerable to the routing attacks of jamming and tampering. For example, jamming attack transmits a noise signal continuously to confuse the normal radio signal. Some of the jamming attackers only generate the noise signal, when a particular legitimate node starts to use the radio device [6]. In addition, in some remote areas the attackers have ability to tamper with the device, due to the insecure installation and can extract the secret information.

In MAC layer, many types of attacks can be launched, for example Denial of Service (DOS) and MAC target attack like spoofing and MAC jamming [7]. When the device installed with a single interface, the DOS attacks transmit the spurious packets and keep the channel of device busy always. This

results in high energy consumption and interrupting the legitimate device communication in the network. The MAC layer is affected by the passive layer attack such as traffic analysis.

In the first way, the attackers can initiate the route discovery process maliciously with the destination IP address, but it does not belong to the network. Thus, the RREQ is broadcast continuously until the Time To Live (TTL) expires, since no one have the route for the destination node with a fake IP address. Another way is to increase the TTL, which highly consumes the node energy in the network, resulting in premature network dead. The significant attacks such as black-hole, gray-hole, and worm-hole target the data forwarding phase. A black hole node is an attack and it brilliantly attracts the data flows in the network through it by always giving a positive response to forward the packets to the destination. After initiating the transmission, the black-hole attackers drops all the packets routed through it. A gray hole is a variant of the black-hole attackers, since it partially drop the data packets. A worm-hole attack makes tunnels with other attack and these colluding devices disrupts the packet routing by dropping the packets.

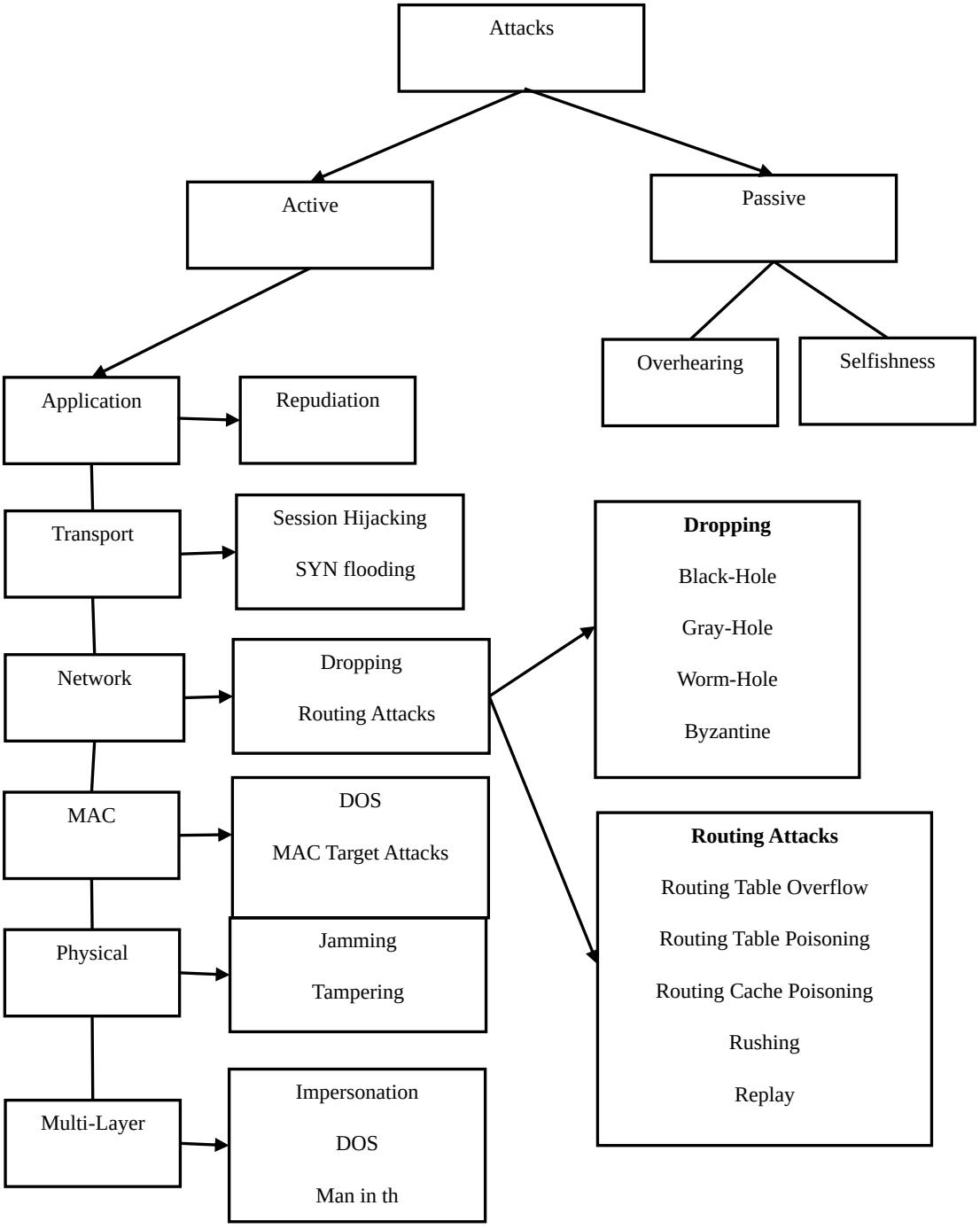

Figure 1: Classification of Attacks at various Layers of MANET

The transport layer is vulnerable to the variant of DOS attack such as SYN flooding attack. The attackers transmit a request of SYN towards the target node and create a large number of traffic flows with legitimate node. It consumes a lot of battery energy to make a system to dead soon.
The repudiation attack denies the activities performed at the application layer. Moreover, the application layer is also vulnerable to the viruses, worms and malicious codes.

2.1 Risk of Multi-Layer Attacks

Multi-layer attacks can exist in any layer of the network and, impersonation and DOS are the examples of multi-layer attack in MANET. The impersonation attacks are launched by spoofing or compromising the legitimate devices in the network [10,11]. The attackers exploit the identify of others, such as MAC address as well as the IP address used in the network layer. The nature of the wireless medium eases the attackers to spoof the MAC identifiers. Once the attackers spoof the MAC address, the detection systems are failed. Since, the security weakness of conventional detection systems in MANET is the consideration of MAC addresses in detecting attacks. Moreover, the impersonation attack is the primary step to carry out further network attacks with the aim of disturbing the network activities. According to the usage of impersonated nodes in the network activities, the attackers can reconfigure and remove the security measures and thus other attacks can easily attack the network. For example, the Sybil attack can be launched in the network with the support of impersonation attack.

The Sybil attacker participates in the route discovery phase to locate it in different routing paths between a single source and destination [12]. In this way, the attacker compromises other nodes and, creates routing loops as well as dead ends in the alternative routes. Under the Sybil attack, an attacker can exploit one or more fake or others identities to disturb and deteriorates the network performance. If the communicating devices authenticate each other using predetermined cryptographic mechanism, the Sybil attacks can be prevented by the intrusion detection systems. Instead of partial compromization, if the Sybil attackers compromise all the secrets of legitimate devices the attackers are free to perform the malicious activities even if the nodes are authenticated using cryptosystem. Using the impersonation attack, another attack entered into the network is invisible node attack. In a MANET, the communication is established using the route request broadcasting. This leads the MANET routing protocols subject to the Invisible Node attack. The invisiblenode is involved in the packet routing without revealing its presence in the path. The invisible node silently involves in data forwarding and misleads the source node. The conventional cryptographic authentication mechanisms, either symmetric or asymmetric key encryption fail to identify this type of attack on the wireless communication.

The stolen identity attack attempts to steal the credentials of legitimate nodes like identity and secret certificate keys. When the malicious nodes update the stolen credentials using the authority, the legitimate nodes are marked as attackers and moreover, it is not a valid member in the network. In this way, only the stolen identify attackers can use these stolen credentials and so the cryptographic authentication techniques fails to deal with the Sybil, invisible, and stolen identity attackers. Moreover, the impersonation leads to the complete device cloning, which is more severe than impersonation. Cloning refers the device programming, in which the hardware address of the device is changed. This is called licensed services or authorized medium access. Therefore, the risk induced by the impersonation attack is critical, since the attack can materialize into several attacks in the network.

2.2 Survey on Defense Mechanisms against Attacks

Several defense mechanisms have been proposed against different types of attacks in MANET.Generally, the defense mechanisms can be categorized into proactive and reactive as shown in figure: 2

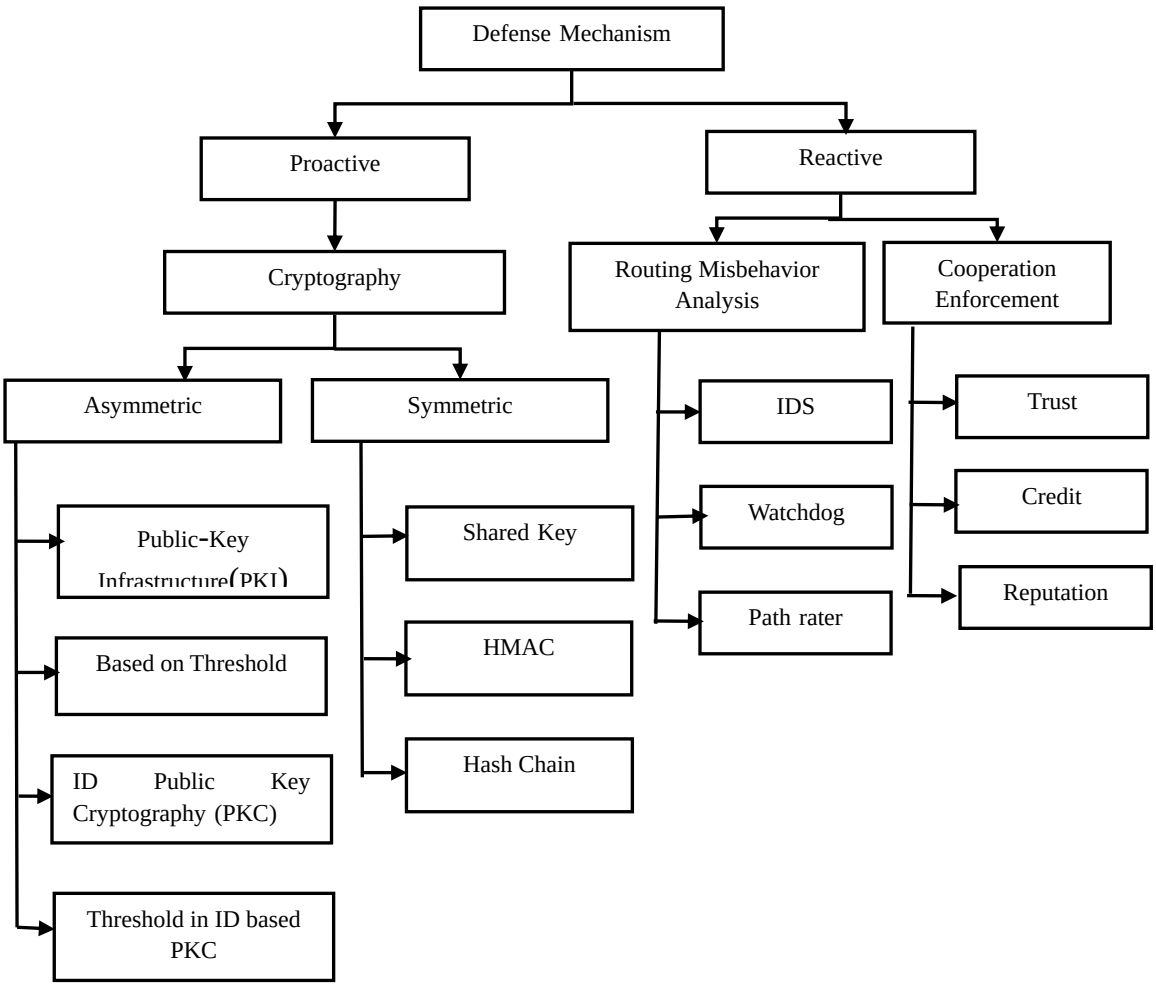

Figure 2: Defense Mechanisms against Attacks in MANET

The defense techniques which are deployed proactively before the launching the attacks in the network are called as proactive defense systems, whereas the reactive defense techniques come into action during an attack [2]. In reactive defense systems, the cooperative enforcement techniques are most suitable for active routing attacks of network layer in MANET. In order to enforce the cooperation of nodes in routing, the trust or some credits are provided to the nodes according to their routing behavior. The cooperation enforcement measurement is an essential module in the reactive security system. The trust refers the belief level of a node based on the routing performance.

The trust management maintains and updates the trust values by monitoring the routing behavior continuously. In order to improve the routing performance, several security mechanisms have been proposed to measure and select highly trusted nodes. Highly trusted node means the good personal routing experience and so it is involved in the data routing. For low trustworthy nodes, the packets are restricted to route in the network.

The defense models such as IDS, Watchdog, and Path rater model analysis the routing behavior in past communications. Watchdog aims at improving the routing performance even in the presence of attackers in the network. Path rater assists to determine the route that is free from attacker nodes. The watchdog system maintains a counter that counts the failure rate of communications. It increases the count when its next hop refuses to route the data packets in a discovered path. However, these techniques are failed in the following cases: network collision, limited transmission range, false misbehavior, and gray hole attack.

2.3 Defense System against Routing Layer Attacks

The routing layer active attacks such as black-hole, gray-hole, and worm-hole drops the packets and deteriorates the network performance [13-18]. The malicious nodes send a positive response to the sender node during the route discovery process, or it replies the sender node using route reply messages; however the attacker has no shortest path to the destination through it. By enabling the watchdog in every Mobile node in the network, the routing activities of neighboring nodes is continuously monitored. The continuous dropping of data packets by a node indicates the black-hole attack behavior and the node is isolated from the network. Some of the conventional defense techniques identify the black-hole attackers in route discovery phase using sequence number. Since, the black-hole attack attracts the sender node in route discovery process by assigning the sequence number which is too larger than others, the black-hole attackers can be identified easily.

The Collaborative Contact based Watchdog (CoCoWa) system includes watchdog as well as information diffused in the

identification of selfish or packet dropping attacks [19]. The watchdog node continuously monitors the routing involvement of a node and generates the opinion for each and every event for a node according to its trustworthiness. The watchdog system can identify the black-hole attackers, but it fails to detect the collaborative black hole and gray hole attackers. Flooding attacks initiate the route discovery process with fake destination address into the network. The main purpose of flooding attack is energy and bandwidth wastage. Several filtering schemes have been used for secure MANET. All the neighboring nodes of a source node watch the packet generation rate and store it. After a certain interval, it is marked as a flooding attack when a source node exceeds the threshold of routing packet generation. After that, the routing packets forwarded by the marked nodes are discarded by the neighboring nodes. However, the reactive defense techniques fail to discover the multi-layer attacks such as impersonation.

2.4 Defense System against Multi-Layer Attacks

The network protocols exploit cryptography techniques in the provision of data security such as authentication, data confidentiality, and integrity over the MANET. However, the cryptographic defense systems do not assure the security of MANET against black-hole, gray-hole, and worm-hole attacks. Moreover, some secure routing protocols assume that the nodes already implements the certificate based authority in the network using encryption algorithm.

Table 1: Comparative of Security Solution in MANET

Secure Protocol	Detected Attacks	Mechanism	Limitations
Authenticated Routing for Ad Hoc Networks (ARANA) [32]	Malicious Packet Manipulation	Cryptography	Certification authority requires more energy Inefficient protection, due to the usage of public key
Secure Adhoc On Demand Distance Vector (S-AODV) [33]	Malicious Packet Manipulation and impersonation	Cryptography	Public key cryptography induces high overhead
Improved version of Secure Efficient Ad hoc Distance Vector Routing (I-SEAD) [34]	Routing Update	Cryptography	Handling limited attacks only
Security-Aware Ad hoc Routing(SAR) [35]	Malicious Route Discovery	Cryptography	Certification authority requires more energy
Position-Aware Secure, And Efficient Mesh Routing (PASER)[36]	Worm-Hole And Cryptography Attacks	Cryptography And Location	Gps Hardware Increases The Detection Cost
Secure Routing Protocol Against Wormhole Attacks In a Sensor Network (SERWA)[37]	Worm-Hole	Cryptography And Reputation	Possibility Of Distributed Key Hacking Is High
Leak-detector[38]	Black and Gray-hole attack	Statistical Model	Integration of existing protocol increases the complexity
Collaborative Routing Protocol (CRP)[38]	Black, Gray-Hole, and Tampering	Statistical Model	During high collision, the statistical model may fail

Aside from cryptography based multi-layer security, two types of security solutions are used in handling some of the multi-layer attacks, such as DOS, hardware and statistical-based solutions. The hardware-based security solutions utilize GPS or an antenna to verify the location information provided by a node. To avoid the impersonation, some of the conventional IDS works, exploit fingerprints of physical medium like signal strength to identify the impersonation attacks in physical layer. Unlike hardware based solutions, the software based security solutions track the nodes to record their successful past communication with neighbors and selects highly trusted next hop for routing. Table 1 describes some of the defense systems against single as well as multi-layer attacks with its limitations.

3. CRYPTOGRAPHY BASED SECURITY AGAINST IMPERSONATION ATTACK

Mostly, the cryptographic algorithms are used in providing security against impersonation and modification attacks at multiple layers [20-31]. Cryptography solution can be classified into Asymmetric and Symmetric solutions. The asymmetric solution is also known as public-key cryptography. This technique exploits public and private keys to ensure the secure transmission. The public key of a node is visible to all other nodes in the network; however the private key is kept secret. One of the widely used public key cryptography is RSA. The symmetric cryptography exploits same key for both encryption and decryption. In practice, keys are shared secret between two nodes that communicate with each other. The symmetric solution has to share a secret key to encrypt and decrypt the message, but once the key has leaked, the symmetric encryption technique will fail.

HMAC implements the message authentication code with a combination of the secret key and hash function in MANET. Most of the security solutions exploit the hash functions such as MD5 or SHA-1. It ensures that the transmitted data containing its original data without modification using a secret key. In credential protection scheme, the hash chain algorithms have been used widely in MANET. There is no possibility to reverse the hash function; due to the hash function has one-way property. The hash function limits the length of chain, and it uses only the reverse order of generation. For example, the examples of protocols that use one-way key chains are SAODV, ARIADNE, and LEAP in MANETs.

The public key cryptography, PKC needs to authenticate the public keys. Otherwise, hacking of a public key by the attacker is easy. In conventional, some trusted frameworks have been proposed to ensure the public key ownership. In secure communication, the nodes that want to establish the communication has to exchange the public keys in a secure manner. However, the public key authentication is not a scalable solution. In case of infrastructure support, the trusted third party can be used to distribute and authenticate the public keys in the network. However, in MANET, it is not possible. There are two models used in PKC such as centralized, web-of-trust, and decentralized models. In order to extend the scalability of the centralized PKC model, the hierarchical models have been used by the entities. The decentralized is vulnerable to cryptography attacks in MANET, due to the lack of well trusted security model. Thus, some works distribute the central trust value to multiple authorities using any secret sharing scheme. For further security, the cryptographic scheme distributes the public key to all, but the private key is divided into multiple and each piece is shared to more than one entity in the network.

3.1 Key Management Schemes in Cryptography Solutions

Conventionally, several key management schemes have been proposed in MANET. Most of them exploit public key cryptography model, since it retains and authenticates the key in multiple locations which ensures further security in cryptography solutions. Threshold cryptography is another familiar security model in PKC. With this security model, the network can tolerate the attacks, until compensating t-1 legitimate nodes in the network. Some of the conventional key management schemes take advantage of both the central and fully distributed trust models and ensures the security in MANET. High complex key management is not suitable for resource constraint nodes, and so the symmetric key cryptography models exploit distributed key management schemes. In which, the keys are pre-loaded in a large key pool. The key pattern should ensure that one key should be allocated for only one node, and moreover a common key should not be used by the group of nodes in the network. For MANET group communication, one key is shared among group of nodes secretly. However, it is not much secure in group communications.

The main advantage in Identity based Cryptography (IBC) is the piggybacking concept, i.e. the identity value is kept in message, however this leads to the problem of identity exposure. It is very dangerous in military environment. For example, if a commander wants to share his identity with a soldier, but it is overheard by the attacker, the secret communication between the commander and soldiers are leaked and enemies are alerted. The traffic analysis is a mainly used tool by the attacker and it is possible by the attack of eavesdropping. In order to prevent the traffic analysis, the secure wireless communication exploits anonymity. Anonymity defines the state of being not identifiable and it is selected within a set of subjects that is called as anonymity set. Some of the solutions tackle this problem by proving group public key and individual private key. This reduces the control overhead and ensures the better routing performance. Moreover, each time a node can leave or enter into the network, thus periodic refreshment in group key management is essential.

The MOCA assigns current trust value based on the number of hops and freshness of the cached route in a routing table. However, the securing the route discovery process is complex, since most secure routing protocols rely on the establishment of a secure key sharing service in advance. The Secure and Efficient Key Management (SEKM) is a decentralized key management scheme in MANET. Like other decentralized key management systems, the secret certificates area shared to a set of nodes, not for a single node, since dependency on a single node in MANET is not fair for security.

4. CONCLUSION

The rise of wireless communication usage in real time environments has increased the necessary of security. The cryptography has been used as the solution to success the secure communication in MANET. In order to clearly demonstrate the impact of impersonation attack on multiple layers over MANET, this work conducts a survey on network attacks and conventional cryptography security solutions. Beside the single and multi-layer attacks and its solutions, key management issues in symmetric, asymmetric and group key solutions are discussed. Although several works have been proposed against impersonation attacks already, there is a

scope on the research of MANET security. However, there must be a tradeoff between security and routing performance, and it is necessary to mitigate the impersonation attack on other layers.

5. REFERENCES

[1] Nie, Pin. "Security In Ad Hoc Network.", 2006.

[2] Wu B, Chen J, Wu J, Cardei M., "A Survey Of Attacks And Countermeasures In Mobile Ad Hoc Networks", In Wireless Network Security, Springer, Pp. 103-135, 2007.

[3] Daza V, Herranz J, Morillo P, Ràfols C., "Cryptographic Techniques For Mobile Ad-Hoc Networks", Computer Networks, Vol.51, No.18, Pp.4938-50, 2007.

[4] Anantvalee, T., & Wu, J "A Survey On Intrusion Detection In Mobile Ad Hoc Networks", In Wireless Network Security, Springer, Pp. (159-180), 2007.

[5] Zhang, C., Zhu, X., Song, Y., & Fang, Y, "A Formal Study Of Trust-Based Routing In Wireless Ad Hoc Networks", Ieee Infocom, Pp. (1-9), 2010.

[6] Martinovic, I., Pichota, P., Schmitt, "J.B.: Jamming For Good: Design And Analysis Of A Crypto-Less Protection For Wsns", In: Proceedings Of The Second Conference On Wireless Network Security (Wisec) (March 2009).

[7] Balarengadurai, C. And Saraswathi, S., "Comparative Analysis Of Detection Of Ddos Attacks In Ieee 802.15 For Low Rate Wireless Personal Area Network", Procedia Engineering, Vol.38, Pp.3855-3863, 2012.

[8] Kannhavong, Bounpadith, Hidehisa Nakayama, Yoshiaki Nemoto, Nei Kato, And Abbas Jamalipour. "A Survey Of Routing Attacks In Mobile Ad Hoc Networks" ,Ieee Wireless Communications, Vol. 14, No. 5, Pp. 85-91, 2007.

[9] Nadeem, Adnan, And Michael P. Howarth. "A Survey Of Manet Intrusion Detection & Prevention Approaches For Network Layer Attack.", Ieee Communications Surveys & Tutorials, Vol.15, No. 4, Pp. 2027-2045, 2013.

[10] Pal, Sarit, Asish K. Mukhopadhyay, And Parthapratim Bhattacharya. "Defending Mechanisms Against Sybil Attack In Next Generation Mobile Ad Hoc Networks." ,Iete Technical Review 25.4 (2008): 209-215.

[11] Goyal P, Parmar V, Rishi R. "Manet: Vulnerabilities, Challenges, Attacks, Application", Ijcem International Journal Of Computational Engineering & Management,2011 .

[12] Grover, Jyoti, Manoj Singh Gaur, And Vijay Laxmi. "A Novel Defense Mechanism Against Sybil Attacks In Vanet", Proceedings Of The 3rd International Conference On Security Of Information And Networks.Acm, 2010.

[13] Awerbuch, B., Holmer, D., Nita-Rotaru, C., & Rubens, H. "An On-Demand Secure Routing Protocol Resilient To Byzantine Failures", Inproceedings Of The 1st Acm Workshop On Wireless Security (Pp. 21-30). Acm 2002.

[14] Deb, N., &Chaki, N., "Tids: Trust-Based Intrusion Detection System For Wireless Ad-Hoc Networks", In Computer Information Systems And Industrial Management Springer, Pp. 80-91), 2012

[15]Pankaj Sharma And Yogendra Kumar Jain, "Trust Based Secure Aodv In Manet", Journal Of Global Research In Computer Science, Vol. 3, No. 6, 2012

[16] Dalal, R., Khari, M., & Singh, Y, "Survey Of Trust Schemes On Ad-Hoc Network", In Advances In Computer Science And Information Technology.Networks And Communications, Springer, Pp. 170-180, 2012.

[17] Amiri, E., Keshavarz, H., Heidari, H., Mohamadi, E., &Moradzadeh, H., "Intrusion Detection Systems In Manet: A Review", Procedia-Social And Behavioral Sciences, 129, Pp. 453-459, 2014

[18] Khan, M. S., Jadoon, Q. K., & Khan, M. I. "A Comparative Performance Analysis Of Manet Routing Protocols Under Security Attacks", In Mobile And Wireless Technology 2015 (Pp. 137-145). Springer Berlin Heidelberg, 2015.

[19] Hernandez-Orallo, E., Serrat, M. D., Cano, J. C., Calafate, C. T., & Manzoni, P., "Cocowa: A Collaborative Contact-Based Watchdog For Detecting Selfish Nodes", 2014

[20] Kim,Y., Perrig, A., And Tsudik, G. " Simple And Fault-Tolerant Key Agreement For Dynamic Collaborative Groups", Technical Report 2, Usc Technical Report 00-737, 2002

[21] Kim, Y., Perrig, A., And Tsudik, G "Simple And Fault-Tolerant Key Agreement For Dynamic Collaborative Groups", In 7th Acm Conference On Computer And Communications Security, Pp. 235-244, Acm Press,2000.

[22] Steiner, M., Tsudik, G., And Waidner, M "Cliques: A New Approach To Group Key Agreement. Ieee Transactions On Parallel And Distributed Systems",2000.

[23] Cocks, C. "An Identity Based Encryption Scheme Based On Quadratic Residues.In Proc. Ima Conference On Cryptography And Coding", Lncs, Springer,Pp. 360–36,2000.

[24] Hubaux, J., Buttyan, L., And Capkun, S. "The Quest For Security In Mobile Ad Hoc Networks", In Proc. Of The Acm Symposium On Mobile Ad Hoc Networking & Computing , 2001(Mobihoc 2001).

[25] Capkun, S., Buttya, L., And Hubaux, P "Self-Organized Public Key Management For Mobile Ad Hoc Networks", Ieee Trans. Mobile Computing, Vol. 2, No. 1, Pp. 52-64,2003.

[26] Chen, L., And Kudla, C." Identity Based Authenticated Key Agreement Protocolsfrom Pairings", Tech. Rep. Hpl-2003-25, Hewlett Packard Laboratories, Feb. 12 2003.

[27] Clausen, T., And Jacquet, P. Rfc3626 " Optimized Link State Routing Protocol (Olsr), 2003.

[28] Rafaeli, S. And Hutchison, D. (2003). "A Survey Of Key Management For Secure Group Communication", Acm Computing Surveys, Vol. 35, No. 3, Pp. 309-329.

[29] Sherman, T. And Mcgrew, A. "Key Establishment In Large Dynamic Groups Using One-Way Function Trees", Ieee Transactions On Software Engineering, Vol. 29, No. 5, Pp. 444-458, 2003.

[30] Chien, H.-Y., And Lin, R.-Y. "Identity-Based Key Agreement Protocol For Mobile Ad-Hoc Networks Using

Bilinear Pairing", In Proc. Sensor Networks, Ubiquitous, And Trustworthy Computing , Ieee, Pp. 520–529, 2006.

[31] Chien, H.-Y., And Lin, R.-Y " Improved Id-Based Security Framework For Ad Hoc Network", Ad Hoc Network ,47–60, 2002..

[32] D. Benetti, M. Merro, And L. Vigan`O, "Model Checking Ad Hoc Network Routing Protocols: Aran Vs. Endair A," In Proceedings Of The 8th Ieee International Conference On Software Engineering And Formal Methods (Sefm '10), Pp. 191–202, September 2010.

[33] S. Lu, L. Li, K.-Y. Lam, And L. Jia, "Saodv: A Manet Routing Protocol That Can Withstand Black Hole Attack," In Proceedings Of The International Conference On Computational Intelligence And Security (Cis '09), Pp. 421–425, Beijing, China, December 2009.

[34] C. H. Lin, W. S. Lai, Y. L. Huang, And M. Chou, "I-Sead: A Secure Routing Protocol Formobileadhoc Networks," Multimedia And Ubiquitous Engineering, Vol. 1, No. 1, Pp. 102–107, 2008.

[35] M. O. Pervaiz, M. Cardei, And J. Wu, "Routing Security In Ad Hoc Wireless Networks," Network Security, Pp. 117–142, 2010.

[36] M. Sbeiti, A. Wolff, And C. Wietfeld, "Paser: Position Aware Secure And Efficient Route Discovery Protocol Forwireless Mesh Networks," In Proceedings Of The 5th International Conference On Emerging Security Information, Systems And Technologies (Securware '11), Pp. 63–70, Saint Laurent Du Var, France, August 2011.

[37] S.Madria And J. Yin, "Serwa: A Secure Routing Protocol Against Wormhole Attacks In Sensor Networks," Ad Hoc Networks, Vol. 7, No. 6, Pp. 1051–1063, 2009.

[38] H.-M. Sun, C.-H.Chen, C.-W.Yeh, And Y.-H. Chen, "A Collaborative Routing Protocol Against Routing Disruptions In Manets," Personal And Ubiquitous Computing, Vol. 17, No. 5, Pp. 865–874, 2013.