IJCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Volume-5, Issue-5 E-ISSN: 2347-2693

An Exhaustive Survey on Security Solutions in MANETS

K.B. Kalambe[1*], S.M. Apte[2]

[1]Dept. of Computer Application, Shri Ramdeobaba College of Engineering and Management, Nagpur, India
[2]Dept. of Computer Application, Shri Ramdeobaba College of Engineering and Management, Nagpur, India

Corresponding Author: kalambekb@rknec.edu

Available online at: www.ijcseonline.org

Received: 20/Apr/2017, Revised: 28/Apr/2017, Accepted: 21/May/2017, Published: 30/May/2017

***Abstract*—** Wireless ad-hoc network is a self arranged wireless network comprised of large number of self controlled sensor nodes or mobile nodes. These self controlled nodes are randomly distributed in a decentralized network. These nodes connect with others node using the connectionless links. They have no information about location of other nodes. They are communicating with each other by sensing the position of every other node. They can sense within some specific transmission range. They possess the non uniform structure. Because of their non uniform structure and decentralized nature, wireless network may prone to various attacks so secure routing in wireless network is a critical task. It may consist of some trusted node or it may contain some malicious node, so it is difficult to detect whether the packet is forward to trusted or malicious nodes. So for this kind of problem several security techniques have been proposed. But a full proof protocol is yet to be discovered to handle all the attacks in an integrated manner and therefore still it is a challenge for new researchers. In this survey paper, various existing security protocol have been discussed in details. This Paper is a survey about what are the various types of attacks can occur in routing Protocol and how the security technique is followed in a particular protocol.

***Keywords*—** *WSN, Routing protocol, security, attacks, malicious node, packet*

I. INTRODUCTION

Wireless network is a self configurable network that consists of collection of sensor nodes or mobile nodes, where each node works independently and do not need the support of any existing network framework. Self configurable network means that a node connects or disconnects with other nodes automatically at any point in time without informing to other nodes and they are movable as also irrespective of distances between them. Forwarding data from the source to destination needs proper node discovery where each node acts as a intermediate node or relay agent to send the data. Each node adjusts the topological parameters and reconfigures as per need due it its highly effective communication capabilities. Fast organization of the ad hoc network is also possible as each node is capable of directly connecting the network using wireless communication link with the neighboring node if it belongs to transmission range. The topology being random, it broadcasts route discovery packet at runtime to discover nearby node easily. But the major resource constraint is the availability of restricted energy, restricted battery and restricted transmission range, due to which the functionality of the network may get affected. The Dynamic structure allows the networks to be accessed by all types of users-opponent or adversary and hence highly prone to network attacks.

A. Need of security in Adhoc Networks:

The dynamic structure of ad hoc networks makes it more vulnerable to different kinds of attacks at different layers. Due to mobility of node in network, it can connect or disconnect a network anywhere at any instant of time without informing other nodes. Even an adversary node can easily connect to the network and make use of available network resources like wireless links, energy levels. An adversary uses this vulnerability to know about the network and then attack the network also it may eavesdrop the confidential communication between source to destination. To overcome this security issue we need to first understand the limitations of wireless network environment. In this type of network, there is no centralized server available to control the traffic in a highly dynamic and large scale ad-hoc network so it impedes trust. Also it has limited transmission range and limited resources like- computational power, battery, bandwidth etc. An opponent can unnecessarily block and waste these restricted resources and affect other trusted node nodes. Adhoc network is scalable in nature so that due to highly mobile nodes, number of nodes defining the scale of ad-hoc network changes all the time as nodes move from one zone to another. This changing affects the security mechanism of which the adversary simply takes advantage.

In wireless network, routing protocol assumes that the nodes are authentic and trusted so a malicious attacker can become an important routing agent who can easily disrupt network without getting detected. Due to dynamic topology and changing nodes membership disrupts the trust relationship among nodes. So there is a need of security mechanisms. Also the nodes with limited power supply may behave in a selfish manner and cause several problems. The intruder can even uses its power for its own operation. The communication among nodes is broadcast which means information is given to every node in a network. So any opponent node can utilize this information in a wrong manner.

In wireless network consists of nodes having dynamic energy, different hardware component and running on various software versions establishing communication between these heterogeneous components becomes a bigger challenge. Due to this restricted communication range, within this range opponent can easily attack with malicious intentions. If routing protocol uses cryptography its performance is affected due to dynamic topology and mobility of nodes also key sharing is a big issue. Due to transmission issues like high bit error rate (BER) in the wireless channel, presence of disturbance, position dependent contention, more collisions due to the presence of hidden terminals, unidirectional links, link breaks due to mobility etc wireless Ad hoc networks causes a much more packet loss. In WSN, our aim to achieve better quality of services such as reliable network, high packet delivery ratio, high throughput, low routing overhead, etc. If Quality of service parameters are good, then your network will be more reliable. But an opponent can easily capable of manipulating the QoS parameter by disturbing the process in the network. Therefore, because of infrastructure less network and malicious attacks, security in ad-hoc network is a challenge.

B. *Malicious behavior of Node:*

Genuine behaviour of a node can be defined as follows "When any function in an ad hoc network is performed between source node (S) and destination node (D) by assuring the security principles of Confidentiality, Integrity, Availability, Authenticity and Non-Repudiation, then it is called the Genuine Behaviour of a node."

Malicious Behaviour- "When any node disturbs the above mentioned security principles, such nodes are considered as malicious". This adversary node performs many malicious activities such as it will drops the packet or simply consumes it and does not forward it or it will perform unnecessarily operations and waste the battery or it may consumes the bandwidth such that no other legitimate node can use it. It can simply eavesdrop the confidential communication. Genuine updates cannot be stored in the buffer because this malicious node may be fill buffer with fake updates. Opponent Node can be enter without authentication and Stale Packets injected to create confusion in the network or it can restrict the two trusted nodes from communicating or tamper the content of the packets to change it completely. Opponent node can denied from sending message to other destination node. It will encounter wrong routes to the legitimate nodes to get the packets or to disturb the operations and it will isolate the node from taking part in network operation or create delays if source node reroute the packet by alternate route. Malicious node may steal the information such as the location, content, sequence number to use it for further attack. When two trusted nodes communicate, a opponent node captures their session to get some meaningful information from their conversation.

C. *Types of attacks:*

WSN are vulnerable to attacks at different levels. The attacks at two different levels are attacks that occurs on the basic mechanisms of routing and attack that damages the security mechanisms. These attacks can be further classified as internal and external depending on where they occur i.e. from within the network or from outside.

- Internal Attacks: Attacks which are directly on nodes presents within network and links interface between them comes under internal arracks. These attacks occur when wrong routing information is broadcast to other nodes. They are more difficult to handle as identifying malicious nodes is big challenge due to dynamic topology.
- External attacks: Malicious node can enter anywhere at any time in the network so they prevent the normal communication of network by causing network congestion, denial of services (DoS), and broadcasting wrong routing information etc or producing additional overhead. External attacks can be further divided as: Passive attack and Active Attack.

The paper is organized as follows. Section II deals with the exhaustive study and research that has taken place in the domain. Section III explores layer wise attacks in the tabular. In section IV different security solutions that have been incorporated have been discussed .Section V puts forth a conclusion, after proper study of different existing protocols has been made prior to it.

II. Literature Review

Vulnerability is a major weakness in every security system. MANETs are more vulnerable than wired network, as they are infrastructure less and any node can join the network at any point in time. This system may be prone to unauthorized data manipulation, if the system does not verify a nodes or user's identity before allowing data access. These vulnerabilities can be challenges and issues of MANET security. Decentralized management, availability of Resource, Scalability, Cooperativeness, Dynamic topology, restricted power supply, Bandwidth constraint, No predefined Boundary and many such challenges make Manets more vulnerable to external attacks. The authors in [1] have enhanced the existing AODV protocol with some security extensions added to them and have put forth new protocol SE-AODV for efficient and secure routing. This new SE-AODV adds extra features to same AODV routing protocol making path formation more secure and followed by evaluation of proposed algorithm performance by comparing it to SAODV. But the major issue is how to detect and deal with a malicious node has been the key area of research .this has resulted in some scenarios wherein the node was malicious right from the beginning even before it joined the network, or initially it was a good node but after lapse of some time it has started its malicious activity, or maybe it pretends to be authentic but by helping another malicious node it is doing wrongful activities. None of possibilities can be identified in the beginning, unless the first packet is dropped at the node [2]. Even there are several reasons for the dropping of the packet and every packet drop at any particular node cannot be treated as the confirmation that the node is adversary node. Hence Detecting and Dealing with Malicious Nodes is a big problem in MANET. Similarly effect of varying node mobility can be predominantly seen in the analysis of the various routing algorithms [3].These adversary nodes give rise to various attacks like black hole attack, wormhole attack , sinkhole attack , jelly fish attacks etc that disrupts the network traffic . This results in high packet drop rate and eventually retransmission of the packets further results in network overhead. This results in the queuing mechanism to be implemented in Manets too as discussed in [4]. A survey of different scenarios suggests various attacks, their bifurcation in wireless networks and efforts need to be taken for their analysis under different scenarios in [5]. Due to installation of wireless access points or devices in an open environment, Wireless attacks are more vulnerable and next generation researchers will need to come up with more intelligent and stronger security mechanisms and make a safer network. Apart from the nature of attacks there is another view point that needs to be considered. At different layer the nature of attacks vary and so their solution [5, 6, 7]. So no particular protocol will be able to provide a complete solution. In the presence of malicious nodes, one of the main objectives of MANET is design a robust security solution that can protect MANET from various routing attacks in totality. However, these solutions are not efficient as for MANET resource constraints, i.e. battery power and limited bandwidth need to be considered too. Mobile ad-hoc network can operate in isolation or in coordination with a wired infrastructure. Hence there is a need for flexibility along self organizing facilities which on one hand is biggest strengths of MANET's, as well as their biggest security vulnerabilities. The main focus needs to be on attacks, their solutions and improvement in new protocols [8, 9]. A security analysis is therefore attempted focusing on detailed comparison that can provide insight regarding the applicability of a particular protocol for a specific application domain [10]. The different attacks (active or passive attacks), security challenges, different layers protocols and different security technologies are introduced [11, 12].

Hence an effort has been made to study these various security solution in this exhaustive survey.

III. Layer-wise Attacks in Manets

In MANET, being infrastructure less, there is high chance of security attacks. The three main security goals to be considered are - Confidentiality, integrity and availability.

Attacks threatening confidentiality are:

- Snooping: Unauthorized access and interception.
- Traffic analysis: Monitoring online traffic and obtaining information.

Data integrity is highly endangered by several kinds of attacks like: repudiation, modification, masquerading, replaying. The data availability can be endangered by Denial of Services, while confidentiality is intercepted is done through eavesdropping. Threat analysis and the identified capabilities of the potential attackers makes it essential to study various types of attacks that can occur in different layers of the network in MANETs. These attacks[24,25] affect different properties of information depending on what the opponent is able to access and are discussed in the table below.

The tables below give attacks information as per different layer-wise attacks.

Table 1. Attacks at Physical Layer

Physical Layer attacks			
Security issues	***Sr No***	***Attack Type***	***Characteristics and features***
1)Signal jamming, 2)Denial of Service	1	Eavesdropping	Interception of confidential information
	2	Jamming	Interruption of legitimate transmission
	3	Active Interference	-Changes the order of messages or attempt to replay old messages -Blocks the wireless communication channel -Distorts communications.

Table 2. Attacks at Data Link Layer

Data Link Layer attacks			
Security issues	***Sr No***	***Attack Type***	***Characteristics and features***
1)Protecting Wireless MAC protocol and 2) providing link layer	1	**Selfish Misbehavior Node attack**	-Directly affects self performance of nodes. -Conservation of battery power and gain unfair share of bandwidth. -Refuse to take part in the forwarding process. -Intentionally drops the packets.
	2	**Malicious Behavior**	-Denial of Service (DOS), --Attacks on Network integrity,

Data Link Layer attacks			
security support		**Node attack**	-Misdirecting traffic.
	3	**Traffic Analysis**	-Derive confidential data about network topology -Analyzing network traffic patterns. -Location of nodes -Roles played by nodes
	4	**MAC spoofing**	Falsify MAC address.
	5	**Identity theft**	Steal legitimate user MAC identity.
	6	**MITM attack**	Impersonate pair of communicating nodes.
	7	**Network Injection**	Inject false network commands and packets.

TABLE 3. ATTACKS AT NETWORK LAYER

Network Layer attacks			
Security issues	***Sr No***	***Attack Type***	***Characteristics and features***
Protecting adhoc routing and forwarding protocol.	1	**Black hole Attack**	-Injects false route replies to the route requests. -Advertising itself as having the shortest path to a destination. -Divert network traffic for eavesdropping. -Attract all traffic to perform a denial of service.
	2	***Rushing Attack***	-Act against the on-demand routing protocols. -Compromised node accepts a route request packet and floods the packet throughout the network.
	3	***Wormhole Attack***	-Malicious node tunnels data packet to another malicious node
	4	***Sinkhole Attack***	-Advertises wrong routing information and receives whole network traffic -Modifies the secret information.
	5	***Replay Attacks***	-Injects previously captured network routing traffic. -Targets the freshness of routes.
	6	***Link Spoofing Attacks***	-Broadcasts or advertises the fake route information *-Malicious node manipulates the data or routing traffic*
	7	**Sybil Attack**	-Generate fake identities of number of additional nodes -A Sybil node may create a new identity for itself -Or Steals an identity of the legitimate node.
	8	**Blackmail**	-Propagate messages to blacklist and isolate legitimate nodes.
	9	**Location Disclosure**	-With simpler probing and monitoring approaches discover the location of a node. -Targets the privacy.
	10	**Denial of Service**	-Complete disruption of routing information operation of ad-hoc network
	11	**Routing Table Poisoning**	-Generates and sends fictitious traffic, or mutates legitimate messages -Routing create false entries in the tables -Injects RREQ packet with a high sequence number so that other legitimate RREQ packets with lower sequence numbers are deleted.
	12	***Colluding misrelay attack***	-Multiple attackers work in collusion to modify or drop routing packets.
	13	***Impersona-tion***	-Use other node's identity, such as IP or MAC address.
	14	***Selective Forwarding/ Gray hole Attack***	-Selectively drops the packets coming from a particular node -Stop the packets in the network by refusing to forward -Or drop the messages
	15	***Sleep Deprivation***	-Consume Resources of the specific node/nodes by constantly keeping them engaged in routing decisions. -Consume batteries and network bandwidth obstructing the normal operation of the network
	16	***Node Isolation Attack***	-Isolate a given node from communicating with other nodes. -Prevent link information of a specific node from being spread to the whole network.
	17	***Cloning Attack***	-Adversary captures a few of nodes, replicates them and then deploys arbitrary number of replicas throughout the network. -Clone has the same security and code information of original node.
	18	***Byzantine attack***	-Creating group of compromised nodes and routing loops, forwarding packets through non –optimal paths or selectively dropping packets.
	19	***RERR Generation***	-RERR messages to some node along the path. -Cause breakdown of multiple paths between nodes. -Cause a number of link failures.
	20	***De-synchronization attack***	-Adversary repeatedly forges messages to one or both end points which request transmission of missed frames.

Network Layer attacks			
			-Prevent the end points from exchanging any useful information
	21	***Overwhelm attack***	-Attacker might overwhelm network nodes. -Forward large volumes of traffic to a base station through these nodes. -Attack consumes network bandwidth and drains node energy.
	22	***The Invisible Node Attack***	-A node effectively participates in functioning of protocol without revealing its identity.
	23	***Fabrication:***	-Generate false routing messages or fabricated routing error messages.
	24	**IP Spoofing**	-Falsification of IP address.
	25	**IP Hijacking**	-Impersonation of legitimate user IP Address.
	26	**SMURF attack**	-Paralysation of network by launching huge number of ICMP requests.

TABLE 4. ATTACKS AT TRANSPORT LAYER

Transport Layer attacks			
Security issues	***Sr No***	***Attack Type***	***Characteristics and features***
Authenticating and securing end-to-end communication through data encrypttion	1	**Session Hijacking**	-Attacker node tries to collect secure data (passwords, secret keys, logon names etc) and other information
	2	**SYN Flooding Attack**	-Attacker creates a large number of half opened TCP connection with node and never completes the handshake.
	3	***Man-in-the-middle attack***	-Sniffs any information being sent between two nodes. -Impersonate sender or receiver.

TABLE 5. ATTACKS AT APPLICATION LAYER

Application Layer attacks			
Security issues	***Sr No***	***Attack Type***	***Characteristics and features***
Detecting and preventing viruses , worms, malicious codes and application abuses	1	Malicious code attacks	Attacks include Worms, Viruses, Spywares, and Trojan horses – both on OS and user application.
	2	Repudiation attacks	Refers to a denial of participation in all or part of the communications.

IV. SECURITY SOLUTIONS FOR VARIOUS TYPES OF ATTACKS

There are several security solutions which can be applied through the methods of Cryptography, Intrusion Detection System, Security Protocols, Trusted Third Party (TTP) and several other schemes

A. Security using Cryptography –

In networking, data is made secure using various cryptographic methods .The original data is encrypted and converted into unreadable format and then sent over the network. The intruder is not able to understand content of original message even if he succeeds to accesses the data. Cryptography can be symmetric (which means same key is used to encrypt & decrypt data) and asymmetric (which means one key to encrypt & other to decrypt data). Cryptographic security ensures integrity and confidentiality of data. Various techniques like Digital Signature, MD5 (Message Digest 5), RSA algorithm, SHA (Secure Hash Algorithm), DES algorithm, MAC (Message Authentication Codes) etc belong to this category of cryptographic solutions [13].

B. Security through TTP (Trusted Third Party) –

Here the nodes are provided security by some trusted third party in the form of certificates. In Public Key Infrastructure (PKI) example, a trusted third party also called as Certifying Authority (CA) issues a certificate to only legitimate nodes for preserving authentication security principle. Another third party example is a watchdog node. This watchdog verifies all the nodes for checking their availability. It checks if the packet is forwarded from source through intermediate node to destination node without being dropped, lost or modified [14]. A Random Walker Detector (RWD) is another method for verifying node’s activity to check if the node is under attack or not.

C. Security through Intrusion Detection Systems –

Intrusion Detection System is used to watch malicious behaviour of nodes. Anomaly based IDS identifies the abnormal behaviour in the network i.e. anomaly in the network which confirms an attack. Profile about normal behaviour of a node is maintained in database of IDS which are made under training period. These profiles can either be static or dynamic in nature. IDS can be designed inside a node or it can even work as TTP [15].

D. Security Techniques for Intrusion Resistant Ad hoc Routing Algorithms (TIARA) –

Techniques for Intrusion Resistant Ad hoc Routing Algorithms (TIARA) is a set of design techniques to be incorporated into on-demand routing protocols (DSR and

AODV) in order to mitigate malicious nodes impact and allow acceptable operation of the network .This scheme uses different multi-path routing, source-initiated flow routing, flow-based route access control (FRAC), flow monitoring , use of sequence numbers and referral-based resource allocation and fast authentication. The design principles of TIARA are applied to many existing ad hoc routing protocols to develop solutions resistant to denial of service attacks. Though protocol independent, they require extensive changes to existing protocols for successful incorporation that make them more robust to intrusion attacks [15].

E. Building Secure Routing out of an Incomplete Set of Security Associations (BISS) –

The protocols usually assume that source and the destination must have established security associations with all the intermediate nodes on the routing path. The Building Secure Routing out of an Incomplete Set of Security Associations (BISS protocol) is a set of optimization techniques applicable to participating nodes that have incomplete security associations between themselves [16]. Intermediate nodes are authenticated using their pre-established associations and exchanging public key certificates. The sender or initiator signs the route request packet using its certificate and public key. The certificate is signed by off-line trusted authority. It associates initiator's public key with an identifier, such as the node's address. The trusted authority also certifies public keys of all the participating nodes. BISS works on the assumption that target node of a route discovery process already has an existing security association. The side effect if this scheme is unnecessary increase in number of security associations of unknown node and their distribution over the network.

F. Security using Packet Leashes –

Packet leashes serves as a specific solution which can be combined with functioning of existing protocol to protect against wormhole attacks. It is not a complete protocol but it adds some extra information to each sent packet .This helps the receiving node to analyze whether the packet has travelled unrealistic distance. There are two schemes of packet leashes: temporal & geographical. In temporal leashes, at each node, an outgoing packet is added with extremely precise timestamp [17]. The receiver then authenticates distance travelled after knowing the time taken. All participating nodes require extremely precise clock synchronization which is in order of hundreds of nanoseconds. For highly congested nodes associated with uncertain transmission times, the use of a threshold time synchronization error is required. The second scheme for construction of packet leashes is by using geographical location information and loosely synchronized clocks. At each node, a timestamp and location information of sender obtained using GPS are added with every outgoing packet. The receiver then verifies distance travelled by packet. But all nodes must have appropriate hardware to track their location although clock synchronization need not be as precise as with the temporal method .The only disadvantage of this method is the requirement of extremely precise clock synchronization, or less rigidly synchronized clocks and the knowledge of geographical location.

G. IP-level Security (IPSec) –

IPSec can be used as underlying security mechanism to provide integrity, authentication and confidentiality in mobile ad hoc networks as proposed by several authors. IPSec suite consists of a set of protocols that provide security at Internet Protocol (IP) level.

There are three different protocols –

- Encapsulating security payload (ESP)-added to an IP datagram to provide confidentiality, integrity, and authenticity of data.
- The authentication header (AH) - added to an IP datagram for integrity and authenticity of the transmitted packets. It does not provide confidentiality for the data.
- Internet key exchange (IKE) - protocol that negotiates security association between the two endpoints, exchanges necessary cryptographic keys, and sets up connection configuration parameters.

For implementation of IPSec, the existence of prearranged common secrets between each pair of systems is needed or an online trusted third party (e.g. a certification authority) for validating signed Diffie-Hellman key exchange messages is needed .But in an ad hoc network, neither of the two requirements can be realistically assumed. Other disadvantages of IPSec are –

- Additional configuration overhead.
- Not designed concurrently with the basic protocol.
- Leave unpredictable and undetectable vulnerabilities in the system.
- High level of complexity and lack of documentation hinders attempts at in-depth analysis.
- Cannot guarantee correct operation under internal attacks.

H. Enhancing data security in ad hoc networks based on multipath routing –

Due to varying characteristics of Ad hoc network like dynamic topology, variable capacity links, infrastructure less, etc many issues arise during routing especially when sending a confidential data on one path. Whereas if data is sent on different disjointed paths, it increases confidentiality and robustness as it is almost impossible to obtain all the parts of divided message. Multiple disjointed paths statistically enhance the confidentiality of exchanged messages thereby increasing reliability of data transmission or to provide load balancing. However there is an increase in the routing overhead and other QoS parameters of the network are also affected [20, 21, 22]. Similarly synchronization overhead and security is highly affected.

I. SMT The Secure Message Transmission (SMT) –

SMT scheme works on the concept of establishing Security Association (SA) between the source and destination nodes and operates on an end-to end basis. Here link encryption is not required .The SA between end-nodes provides not only data integrity and origin authentication but it also ensures end-to-end message encryption. Thus it addresses data confidentiality, data availability, and data integrity in network environment. In SMT scheme , each path is continuously given a reliability rating on the basis of number of successful and unsuccessful transmissions for multipath routing .The ratings are evaluated in conjunction with a multipath routing algorithm to find and maintain a secure path and adjust its parameters to remain efficient and effective. SMT primarily focuses on reliability of data transmission. The scheme proposes to use Information Dispersal Algorithm (IDA) in order to divide messages into multiple pieces, each containing limited redundancy and transmitted on a different node-disjointed path. A Message Authentication Code (MAC) is attached and sent with each piece of information in order to provide data integrity and origin authentication [23,24].

J. Jigsaw Puzzle –

This scheme handles data confidentiality and integrity issues in an ad hoc environment. This scheme works with roots of polynomials and breaks the given message into pieces by a jigsaw. It then uses the jigsaw technique. Here the pieces of message are transmitted across multiple node-disjointed paths. Each piece of transmitted message is provided with data integrity and origin authentication by attaching Message Authentication Code (MAC) with each piece of transmitted message. This ensures that no information can be derived unless all of its pieces are known by the adversary. This is based on the concept of All-or-Nothing Transform to a secret message. Multipath routing is when used statistically can enhance the confidentiality of exchanged messages between the sink nodes and destination nodes. For revealing the contents of the secret message, the adversary will need to eavesdrop close to source or destination or he will have to simultaneously listen on all of the paths. This method can be further improvised by if source and destination are made to share a secret prime number which can be used in the message division process. This scheme lacks in data-availability mechanism which reduces its effectiveness in a highly mobile and hostile environment although it provides data confidentiality by using multiple existing paths. This leads to a conclusion that ad hoc network needs a robust solution that efficiently provides with security and lessen the overheads[25, 26].

K. Security implementation using different protocols –

All the above mentioned schemes that are mentioned are capable of handling the security issues only partially and many researchers have proposed different set of protocols with the intent to provide security at different layers. These protocols were designed on the basis of above mentioned schemes with key focus on concept of certification system, cryptography and other security solutions.

In above section, the author describes the previous research works in the form of title, problem statement, objectives, not repeat the information discussed in Introduction [2].

V. CONCLUSION

In this survey, the main focus was to do an elaborate study of various attacks that would arise in a network to make insecure your network. In this paper we describe what type of attacks can be exist at different layers and also what type of security solution exist to handle a particular attacks if occurred. No particular scheme or protocol is capable of handling the various attacks at different layers in the given network .Hence it becomes essential to propose some scheme that is capable of handling at least a majority of attacks and provide a better solution than the existing ones. Hence this effort.

REFERENCES

[1] R. S. Shaktawat ,D. Singh ,N. Choudhary, "*An Efficient Secure Routing Protocol in MANET Security - Enhanced AODV (SE-AODV)* ", International Journal of Computer Applications, Vol.97, No.8, pp.1-12, 2014.

[2] A. K. Gupta, D. Mehrotra, "*Detecting and Dealing with Malicious Nodes Problem in MANET*"- International Journal of Scientific & Engineering Research, Vol.4, Issue.7, pp.61-68, 2013.

[3] A. Vijayan, T. Thomas, "*Anonymity, Unlinkability and Unobservability in Mobile Ad Hoc Networks*", International Conference on Communication and Signal Processing, India pp.3-5, 2014.

[4] PK. Sharma, SL. Mewada, P. Nigam, "*Investigation Based Performance of Black and Gray Hole Attack in Mobile Ad-Hoc Network*", International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.4, pp.8-11, 2013.

[5] G. Kalpana, S. Archana, "*Performance Analysis of Threshold Based Algorithms under Wormhole Attack in MANET*", International Journal of Computer Sciences and Engineering, Vol.3, Issue.7, pp.133-138, 2015.

[6] M. Jamgade , V. Shukla , "*Comparative on AODV and DSR under Black Hole Attacks Detection Scheme Using Secure RSA Algorithms in MANET*", International Journal of Computer Sciences and Engineering, Vol.4, Issue.2, pp.145-150, 2016.

[7] M. Nachammai and N. Radha, "*Survey on Black Hole and Gray Hole Attacks in MANET*", International Journal of Computer Sciences and Engineering, Vol.4, Issue.5, pp.66-70, 2016.

[8] Y. Zeng, R. Zhang, "Active eavesdropping via spoofing relay attack", *2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Shanghai, pp.2159-2163, 2016.

[9] X. Li, H.-N. Dai, Y. Wang, H. Wangt, "*Eavesdropping Activities in Wireless Networks: Impact of Channel*

Randomness", TENCON- IEEE Region 10 Conference, Macao, pp.1-4, 2015.

[10] S. Anusuya, S. Meenakshi, "*An Improved Dynamic Source Routing Protocol for Detection and Removal of Black Hole Attack in Mobile Ad-Hoc Network*", International Journal of Computer Sciences and Engineering, Vol.3, Issue.12, pp.112-117, 2015.

[11] A. Saraf, M. Singh, "*A Trust Proxy Node (TPN) Based Black hole Attack Detection Mechanism in MANET Using AODV*", International Journal of Computer Sciences and Engineering, Vol.3, Issue.12, pp.130-135, 2015.

[12] K. Thamizhmaran, R. S. K. Mahto, V. S. K. Tripathi, "*Performance Analysis of Secure Routing Protocols in MANET*", International Journal of Advanced Research in Computer and Communication Engineering, Vol.1, Issue.9, pp.151-154, 2012.

[13] Usha MK, A.S. Poornima, "*Node-To-Node Authentication Protocol to Prevent Black Hole Attack in AODV*", 2016 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET), *Chennai, pp. 133-136, 2016.*

[14] S.V. Baghel, D.P. Theng, *"A survey for secure communication of cloud third party authenticator*", 2nd International Conference on Electronics and Communication Systems (ICECS), Coimbatore, pp.51-54, *2015*.

[15] R. Ramanujan, A. Ahamad, J. Bonney, R. Hagelstrom, K. Thurber, "*Techniques for intrusion-resistant ad hoc routing algorithms (TIARA)*", MILCOM 2000 21st Century Military Communications Conference Proceedings, USA, pp.660664, 2000.

[16] UK. Singh, SL. Mewada, L. Laddhani, K. Bunkar, *"An Overview and Study of Security Issues & Challenges in Mobile Ad-hoc Networks (MANET)*", International Journal of Computer Science and Information Security, Vol.9, No.4, pp.106-111, 2011.

[17] Y.C. Hu, A. Perrig , D. B. Johnson, *"Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks*", Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies, San Francisco, pp. 1976-1986, 2003.

[18] H. Tran, Hans-Jurgen Zepernick, "*Proactive Attack: A Strategy for Legitimate Eavesdropping*", 2016 IEEE Sixth International Conference on Communications and Electronics (ICCE), Ha Long, pp. 457-461, 2016.

[19] J.A.N. Sidnal, "*Survey - Secure Routing Protocols of MANET*", International Journal of Applied Information Systems , Vol.5, No.4, pp.1-8, 2013.

[20] S. Mewada, UK. Singh, PK. Sharma, "*Simulation Based Performance Evaluation of Routing Protocols for Mobile Ad-hoc Networks (MANET)*", International Journal of Computer Science, Information Technology and Security, Vol. 2, No. 4, pp.728-732, 2012.

[21] D. Airehrour, J. Gutierrez , S.K. Ray, "*GradeTrust: A Secure Trust Based Routing Protocol For MANETs*", 2015 International Telecommunication Networks and Applications Conference, Sydney, pp.65-70, 2015.

[22] S.K. Dhurandher, I. Woungang, I. Traore, "*C-SCAN: An Energy-Efficient Network Layer Security Protocol for Mobile AdHoc Networks*", 2014 28th International Conference on Advanced Information Networking and Applications Workshops, Victoria, pp.530-535, 2014.

[23] UK. Singh, J. Patidar, KC. Phuleriya, "*On Mechanism to Prevent Cooperative Black Hole Attack in Mobile Ad Hoc Networks*", International Journal of Scientific Research in Computer Science and Engineering, Vol.3, Issue.1, pp.11-15, 2015.

[24] Leena Pal, Pradeep Sharma, Netram Kaurav and Shivlal Mewada, "*Performance Analysis of Reactive and Proactive Routing Protocols for Mobile Ad-hoc –Networks*", International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.5, pp.1-4, 2013.

[25] D.D. Punwatkar, K.N. Hande, "*A Review of Malicious Node Detection in Mobile Ad-hoc Networks*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.2, pp.65-69, 2014.

[26] D. Dave, P. Dave, "*An Effective Black Hole Attack Detection Mechanism using Permutation Based Acknowledgement in MANET*", 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI), New Delhi, pp. 1690-1696, 2014.