https://dx.doi.org/10.22161/ijaers/3.12.46 ISSN: 2349-6495(P) | 2456-1908(O)

Literature Survey of Security Enhancement in MANET Routing Protocols of WLANs

Piyush Vyas[1], Neeraj Arora[2], Manish Purohit[3], Ajay Rupani[4]

[1]Ph. D. Scholar, Faculty of ECE, MBM Engg. College, JNV University, Jodhpur, Rajasthan, India
[2]Asst. Prof. & Convener (CS), VMO University, Kota, Rajasthan, India
[3]Asst. Prof. (Sr.), Dept. of ECE Engg., J.I.E.T., Jodhpur, Rajasthan, India
[4]Research Scholar, Dept. of ECE Engg., R.I.E.T., Jaipur, Rajasthan, India

Abstract— *A Mobile Ad-hoc Network (MANET) is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. One of the main issues in such networks is performance- in a dynamically changing topology; the nodes are expected to be power-aware due to the bandwidth constrained network. Another issue in such networks is security - since every node participates in the operation of the network equally, malicious nodes are difficult to detect. There are several applications of mobile ad hoc networks such as disaster recovery operations, battle field communications, etc. The most active research area under MANET routing protocol is security. MANETs have certain unique characteristics that make them vulnerable to several types of attacks. Since they are deployed an open environment where all nodes co-operate in forwarding the packets in the network, malicious nodes are difficult to detect.*

Keywords—MANET, Ad-hoc Network, ARIADNE , CONFIDANT, Secure routing protocols.

I. INTRODUCTION

Mobile Ad hoc networks (MANETs) have several advantages such as ease of deployment, speed of deployment and decreased dependency on a fixed infrastructure. However unique characteristics of MANETs topology such as open peer-to-peer architecture, dynamic network topology, shared wireless medium and limited resource (battery, memory and computation power) pose a number of non-trivial challenges to security design.

Some of the issues and challenges that designer of secure protocols are described in this paper. These issues are analyzed with respect to the primary goals of a secure protocol – confidentiality, integrity and availability, authenticity and non-repudiation. There are many secure versions of MANETs routing protocols are available such as SEAD, ARIADNE, ARAN and SRP which are enhanced version of basic MANET routing protocols. These secure routing protocols are designed to provide security under various types of attacks. However only one cannot gives the security with all aspects so combined strategies are applied.

CHALLENGES IN DESIGNING SECURE PROTOCOLS

This section enumerates the issues and the challenges in designing secure protocols for MANETs [1]:

Shared broadcast radio channel

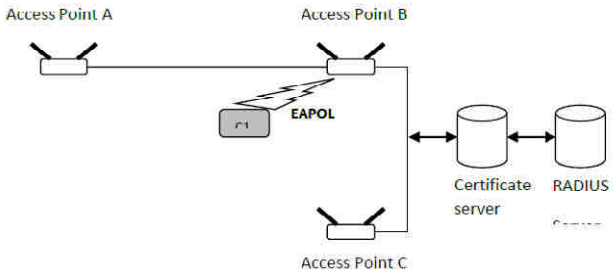
In MANETs, the radio channel is shared by all the nodes by broadcasting the data. Due to this, any malicious node can easily―snoop‖ over the data thereby violating confidentiality in the network. This can be minimized by using a directional antenna.

Hostile environment

MANETs are typically deployed in hostile environments such as battlefield. In such cases, the nodes themselves are prone to attacks. Thus, not only must the protocol address attacks from outside a network, but also the attacks launched from within the network. Such internal attacks are severe and can violate all the goals of security.

Decentralized architecture

In wired networks and wireless infrastructure-based networks (such as Wireless LANs), there is a fixed server which authenticates the users and handles key management. For example, a RADIUS server for authentication and a certificate server for key management may be installed as depicted in fig 1. Here, wireless station C1 sends its authentication credentials to the authenticator (Access Point B) using a protocol such as EAPOL, which in turn forwards the information to the back-end authentication server.



Centralized authentication scheme in Wireless LANs

Such a centralized scheme is infeasible in an ad hoc network due to its distributed nature.

Dynamic Topology

The nodes in a MANET are highly dynamic in nature and hence the topology of the network keeps changing. Due to this the trust relationship between nodes also keeps changing. For

https://dx.doi.org/10.22161/ijaers/3.12.46 *ISSN: 2349-6495(P) | 2456-1908(O)*

example, if any malicious node is detected in a network, its relationship with the surrounding nodes changes. Due to this, the security protocol must also adapt to these changes.

Power limitations

The nodes in a MANET are devices such as PDAs, laptops, etc. which run on batteries. The addition of security ―layers‖ adds more performance overhead and also consumes network bandwidth. One of the severe implications of this is that nodes are easily vulnerable to attacks such as Denial of Service (DoS). Thus the security solution must also be power aware.

II. SECURE ROUTING IN MANETS

This paper primarily focuses on the security issues from a network layer perspective. Several routing protocols for MANETs exist though none of them address the most important issue, namely, security. In order to study the attacks and threats, and to devise a protocol which addresses them, an understanding of the operating environment is needed. The environment can be a managed environment, where a common trusted authority exists such as a RADIUS server or it can be an open environment where there is no a priori trust relationship between the nodes. For example in a battlefield, the nodes have a common trust authority which executes the key management functions. MANETs typically fall in to the open environment type since the nodes are mobile and they establish a connection dynamically. Another possible type of environment is the managed-open environment, where the nodes have already established some security infrastructure. This acts as a starting point for establishing the trust relationship between nodes. Furthermore, the environment can be managed-hostile, which depicts scenarios such as military networks, where security is of prime importance.

Some of the secure versions of MANET routing protocols are described as:

ARIADNE

The ARIADNE routing protocol [1] proposed by Yi-Chun Hu, Adrian Perrig, etc. prevents against several types of active and passive attacks. Active attacks are those where a malicious node eavesdrops on a network and injects fake packets. On the other hand, passive attacks are threats against the confidentiality of the communication rather than the network‘s function. Active attacks can be of several types such as Active-0-1 (in which the attacker owns one node), Active-1-x (in which the attacker owns one compromised node and distributes the cryptographic keys to its x-1 other nodes), and Active-y-x. In addition, an attacker that has compromised nodes is called an Active VC attacker when it owns all nodes through a vertex cut in the network that partitions the good nodes into multiple sets, thereby forcing the good nodes to communicate through the attacker nodes. The wormhole attack is an example of this type of attack.

The ARIADNE protocol is a secure routing protocol based on DSR [14], which withstands node compromise and uses efficient symmetric key cryptography. The assumption made in ARIADNE is that the nodes can authenticate routing messages using three schemes – shared secrets between each pair of nodes, shared secret between the communicating nodes combined with broadcast authentication or by using digital signatures. ARIADNE works in two phases, route discovery and route maintenance similar to DSR. They are in turn described below –

(a) Route Discovery: In order to authenticate the RREQ packets, every source node adds a Message Authentication Code (MAC) computed with the shared key between the source and the destination (KSD). In order to verify the intermediate nodes in a RREQ packet, every node along the path from source to destination authenticates the new information in RREQ packet using a TESLA key [2]. The destination node will buffer the RREP packet until the intermediate nodes can release their corresponding TESLA keys, after which a security condition is met.

Now, the target adds a MAC to the RREP packet hashed with KSD and forwards it on the reverse path to the source node. Further, in order to prevent any malicious node from removing any previous hop from the route, a technique called per-hop hashing is used [3].

(b) Route maintenance: Route maintenance in ARIADNE is similar to DSR, where a node forwarding a packet to the next hop along the source route sends a RERR packet back to the originating node if it is unable to deliver the packet to next hop. The sender node authenticates an RERR packet by checking the time delay in receiving the packet. By using a mechanism such as TESLA, each node that will be able to authenticate the RERR packet buffers it until it can be authenticated.

Ariadne prevents against both active and passive attacks. Specifically it prevents attacks using fabrication such as forming routing loops by spoofing. It also prevents against the black hole attack by using per hop hashing mechanism and many kinds of Denial of Service (DoS) attacks due to flooding of route request packets in the network. Furthermore, it is also efficient since it is based on a reactive protocol which has a better performance than table-driven protocols, and symmetric key cryptography.

CONFIDANT

CONFIDANT [4] (Cooperation of Nodes: Fairness In Dynamic Ad-hoc Networks) is a secure on demand routing protocol for making misbehavior nodes unattractive for other nodes to communicate with. It is based on selective altruism and utilitarianism. It aims at detecting and isolating misbehaving nodes, thus making it unattractive to deny cooperation. Trust relationships and routing decisions are based on experienced, observed or reported routing and forwarding behavior of other nodes. The design of CONFIDANT assumes that the network layer is based on DSR. CONFIDANT consists of the following components: the monitor, the reputation system, the path manager, and the trust manager. Each component takes its function from its name.

https://dx.doi.org/10.22161/ijaers/3.12.46 *ISSN: 2349-6495(P) | 2456-1908(O)*

The monitor is for the neighborhood nodes to record (by listening to other communication) communication between other nodes. The trust manager deals with the incoming and outgoing ALARM messages. ALARM messages are sent by the trust manager of a node to warn others of malicious nodes. The reputation system is mainly used to avoid a centralized rating, local rating lists and/or black lists maintained at each node and potentially exchanged with friends. Similar reputation systems are used in some online auctioning systems. They provide a means of obtaining a quality rating of participants of transactions by having both the buyer and the seller give each other feedback on how their activities were perceived and evaluated. Path manager performs the following functions: i) path re-ranking according to security metric, e.g. reputation of the nodes in the path, ii) deletion of paths containing malicious nodes, iii) action on receiving a request for a route from a malicious node, e.g. ignore, do not send any reply, and iv) action on receiving request for a route containing a malicious node in the source route, e.g. ignore, alert the source. When the monitor detects an anomaly, it informs the reputation system to take an action, which maintains a local ratings list. These lists are potentially exchanged with other nodes; the trust monitor handles input from other nodes. If a list is received from a highly trusted node, the receiver can directly place information from the list into its local ratings list. On the other hand if a list is received from an un-trusted source, the receiver can completely ignore it or give it substantially less weight than a list received from a more trusted node. Finally, the path manager chooses paths from the node‘s route cache based on a blacklist and the local ratings list. The path manager also specifies the reaction to a REQUEST from a node on the blacklist or to a REQUEST that has traversed a node on the blacklist.

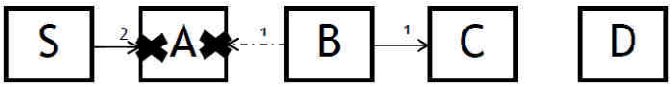
CONFIDANT maintains global reputation values. Each node maintains a single reputation value for every other node with which it interacts, where this value combines all the various functional reputation values. Using global reputations may lead to several other issues [5]. In particular, a global reputation value may enable a node to hide bad behavior with respect to one function by correctly supporting another function. Global reputation values, therefore, do not reveal the importance placed on different services by different nodes. The distributed nature of the mechanism can lead to several inconsistencies in the reputation value. It can also lead to possible attacks on the reputation value such as advertising false high rating or false low rating about another node and negative discrimination (a node refuses services to only some nodes). In general, a simple local reputation mechanism will be more efficient than a complex reputation mechanism.

CORE

Selfishness that causes lack of node activity cannot be solved by classical security means that aim at verifying the correctness and integrity of an operation. CORE [6] suggests a generic mechanism based on reputation to enforce cooperation among the nodes of an ad hoc network to prevent selfish behavior. Each network entity keeps track of other entities collaboration using a technique called reputation. The reputation is calculated based on various types of information on each entity‘s rate of collaboration. Since there is no incentive for a node to maliciously spread negative information about other nodes, simple denial of service attacks using the collaboration technique itself are prevented.

Three reputation systems are used in CORE: subjective reputation, indirect reputation and functional reputation. The subjective reputation is calculated directly from the subject observation. A subjective reputation (direct observation) at time t from the point of view of subject s is calculated using a weighted mean of the observation‘s rating factors, giving more relevance to the past observations. Indirect reputation reflects the value given to the final reputation by the characteristics of the complex societies. Functional reputation is used to apply a function f (which could be a forwarding function, packet function, or any other function) to the subjective reputation value or/ and the indirect value. The function reputation may apply more than one function to the same input and use a third function to get a final functional value.

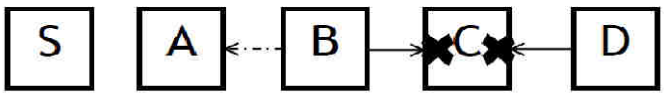
CORE consists of three components: network entity, reputation table and the watchdog mechanism. The network entity comprises of the mobile nodes in the network. Each node is enriched with a set of Reputation Tables (RT) and a Watchdog Mechanism (WD). The RT and the WD together constitute the basis of the collaborative reputation mechanism. These two components allow each entity to observe and classify entities that get involved in a request/ reply process, reflecting the cooperative behavior of the involved parts. The RT is defined as a data structure stored in each network entity. The watchdog mechanism detects misbehaving nodes.



Ambiguous collision

The ambiguous collision problem due to exposed terminal may prevent node A from overhearing transmissions from node B. As Fig 2 illustrates, a packet collision occurs at node A while it is listening for node B to forward the packet. In such a case, Node A will never know if node B ever forwarded the packet. Because of this uncertainty, node A should instead continue to watch node B over a period of time.

In the receiver collision problem, Fig 3, node A can only tell whether node B has sent the packet to node C, but it cannot tell if node C has received it. If a collision occurs at node C, node A only sees that node B has forwarded the packet and assumes that C has successfully received it. Thus, node B could skip retransmitting the packet and evade detection.



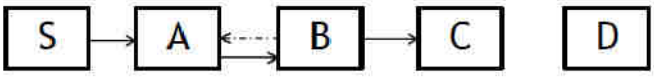
Receiver Collision

https://dx.doi.org/10.22161/ijaers/3.12.46 *ISSN: 2349-6495(P) | 2456-1908(O)*

False misbehavior can occur when nodes falsely report other nodes as misbehaving. A malicious node could attempt to partition the network by claiming that some nodes in the forwarding path are misbehaving. For instance, node A could report that node B is not forwarding packets when in fact it is. This will cause node S to mark node B as misbehaving, whereas the culprit is node A. This behavior, however, is easy to address. Since node A is passing messages onto node B (as verified by node S), then any Acknowledgments from D to S will go through node A to node S, and node S will wonder why it received replies from node D when supposedly node B dropped packets in the forward direction. In addition, if node A drops Acknowledgments to hide them from node S, the node B can detect this misbehavior and report it to D.

Another problem is that a misbehaving node that can control its transmission power can avoid the watchdog [9]. A node could limit its transmission power such that the signal is strong enough to be overheard by the previous node but too weak to be received by the true recipient. Also, a node can circumvent the watchdog by dropping packets at a lower rate than the watchdog‘s configured minimum misbehavior threshold (partial dropping). Although the watchdog will not detect this node as misbehaving, this node is forced to forward at the threshold bandwidth. In this way the watchdog serves to enforce this minimum bandwidth. For the watchdog to work properly it must know where a packet should be in two hops.

Watchdog Mechanism — Many Protocols use watchdog mechanism. Watchdog mechanism has been introduced by [7]. Fig 4 illustrates the working of the watchdog mechanism. Node A cannot transmits all the way to node C, but it can listen the node B‘s traffic. Thus when node A transmits a packet for node B to be forwarded to node C, node A can often tell if node B has transmitted the packet. If encryption is not performed separately for each link, which can be expensive, then node A can also tell if node B has tampered with the payload or the header.



Watchdog Mechanism

The watchdog is implemented by maintaining a buffer to see if there is a match in the packets received and packets forwarded. If so, the packet in the buffer is removed and forgotten by the watchdog, since it has been forwarded on towards its final destination. If the packet has remained in the buffer for longer than a certain timeout, the watchdog increments a failure tally (RT) for the node responsible for forwarding the packet. If a tally exceeds a certain threshold bandwidth, it determines that the node is misbehaving and sends a message to the source notifying it of the misbehaving node. The advantage of the watchdog mechanism is that it can detect misbehaving nodes at forwarding level and not just the link level. The disadvantage is that it might not detect misbehaving nodes in presence of ambiguous collusions, receiver collusions, limited transmission power, false misbehavior, collision and partial dropping [8].

SAODV

The black-hole attack is a killer attack for AODV. In a black hole attack a malicious node acts as an intermediate node, and advertises itself on the shortest path to the destination, which will make the sender node send all the packets through it. The malicious node will then simply drop the packets.

SAODV [13] was introduced to combat the black-hole attack. One solution is to prevent the intermediate nodes from sending a RouteReply message. This is still not good enough because the destination node might select a route that has the malicious node, which will then again drop all the packets.

Also, by not making the intermediate node send a RouteReply message, the delay in the network will increase. To solve this problem the Further RouteRequest message has been introduced in SAODV. When the intermediate node sends a RouteReply message to the source, the source will send a quick Further RouteRequest message to the neighbors of that intermediate node (the RouteReply message will contain information about the next hop on the route). The neighbor node will reply with Further RouteReply message which must contain the intermediate node listed in its route (that has sent the RouteReply message). If it does not, then that neighbor node is a malicious node.

The approach adopted in SAODV is adequate for solving the black-hole problem but it fails to detect the wormhole attacks (when two malicious nodes works together to attack the network).

Authenticated Routing for Ad hoc Networks (ARAN)

Authenticated Routing for Ad hoc Networks (ARAN) [10] is a secure routing protocol based on the AODV protocol. The assumption in ARAN is that every node has a certificate that is signed by a trusted authority. The route discovery and route maintenance mechanisms are based on AODV and elaborated as follows –

Let us assume that a source node S wants to discover a route to destination node D. Also assume that A, B and C are three intermediate nodes on the path from S to D, that their certificates are certA, certB and certC and their private keys are Ka, Kb, Kc respectively. During the route discovery phase, a source node broadcasts a RREQ packet signed with its public key. The packet contains the destination node‘s address D, source node‘s certificate certS, a nonce N and a timestamp t. The nonce and timestamp ensure that the route is fresh. A sequence of route discovery messages is shown below:

S → * : (RREQ, D, certS, N, t) Ks
A → * : ((RREQ, D, certS, N, t) Ks) Ka,certA
B → * : ((RREQ, D, certS, N, t) Ks) Kb,certB
C → * : ((RREQ, D, certS, N, t) Ks) Kc,certC
(NOTE: * denotes a broadcast)

As shown, each intermediate node (such as A, B or C) that forwards the RREQ packet checks the signature(s) of the previous node on the packet by extracting the public key from

https://dx.doi.org/10.22161/ijaers/3.12.46 *ISSN: 2349-6495(P) | 2456-1908(O)*

the certificate. Further, it removes the previous node's signature, signs the RREQ packet with its own private key, adds the certificate to the header and broadcasts the packet to its neighboring nodes. This process continues until the packet reaches the destination D.

D → C : (RREP, S, certD, N, t) Kd

C → B : ((RREP, S, certD, N, t) Kd) Kc,certC

B → A : ((RREP, S, certD, N, t) Kd) Kb,certB

A → S : ((RREP, S, certD, N, t) Kd) Ka,certA

On receiving the RREQ, D will create a route reply (RREP) packet, add the source address S, its own certificate certD, a nonce and a timestamp and sign it with its private key. An intermediate route C on receiving the RREP packet will in turn verify the signature(s) of the previous node. For example, when node B receives the RREP packet from node C, it will verify the signature of node C. It will then remove C's certificate, sign the packet with its own private key Kb, add its certificate certB and unicast it to the next node A on the reverse path as shown above. Nodes B and A will also add a routing table entry to node D indicating that the next hop is C and B respectively.

When node B discovers a broken link to C, it initiates route maintenance as shown:

B → A : ((RERR, S, D, certB, N, t) Kb)

A → S : ((RERR, S, D, certB, N, t) Kb)

Thus it sends a RERR packet, the source node's address, the destination address, its own certificate certB, a nonce and a timestamp signed with its private key to its previous node A. Node A will forward this unchanged to the source node S.

ARAN prevents against attacks which modify the routing information since it uses public key authentication. However, it is vulnerable to DoS attacks which flood the network with fake packets due to the use of certificates which require high bandwidth and processing power of nodes.

SAR

Security Aware Ad-Hoc Routing (SAR) protocol [11] makes use of trust levels (security attributes assigned to nodes) to make informed, secure routing decisions. Current routing protocols discover the shortest path between two nodes. But SAR can discover a path with desired security attributes (e.g., a path through nodes with a particular shared key).

A node initiating route discovery sets the desired security level for the route, i.e., the required minimal trust level for nodes participating in the query/ reply propagation. Nodes at that have the trust level share symmetric encryption keys. Intermediate nodes of different trust levels cannot decrypt in transit routing packets or determine whether the required security attributes can be satisfied, therefore drop all such packets. Only the nodes with the correct key can read the header and forward the packet. So, if a packet has reached the destination, it must have been propagated by nodes having the same trust level.

SAR approach can be extended to any routing protocol. However, it has been presented as an extension of AODV. Most of AODV's original behavior such as on-demand discovery using flooding, reverse path maintenance and forward path setup via RouteRequest and RouteReply (RREP) messages is retained. The RREQ (Route REQuest) and the RREP (Route REPly) packets formats are modified to carry additional security information. The RREQ packet has an additional field called RQ_SEC_REQIREMENT that indicates the required security level for the route the sender wishes to discover. This could be a bit vector. An intermediate node at the required trust level, updates the RREQ packet by updating another new field, RQ_SEC_GUARANTEE field. The RQ_SEC_GUARANTEE field contains the minimum security offered in the route. This can be achieved if each intermediate node at the required trust level performs an AND operation with RQ_SEC_GUARANTEE field it receives and puts the updated value back into the RQ_SEC_GUARANTEE field before forwarding the packet. Finally the packet reaches the destination if a route exists.

In the RREP packet one additional field is also added. When an RREQ successfully traverses the network to the sender, the RQ_SEC_GUARANTEE represents the minimum security level in the entire path from source to destination. So the destination copies this from the RREQ to the RREP, into a new field called RP_SEC_GUARANTEE field. The sender can use this value to determine the security level on the whole path, since the sender can find routes which offer more security than asked for, with which he can make informed decisions.

A major drawback in SAR is that it involves significant encryption overhead, since each intermediate node has to perform encryption/decryption operation. Also, the nodes are classified based on the level of trust. This creates a hierarchical trust based network. SAR evaluates the rust level of routes based only on hierarchy. This hierarchy is predetermined and therefore implies that the trust level of the nodes is static. Furthermore, nodes can spoof each other's trust level. The protocol in general does not scale well.

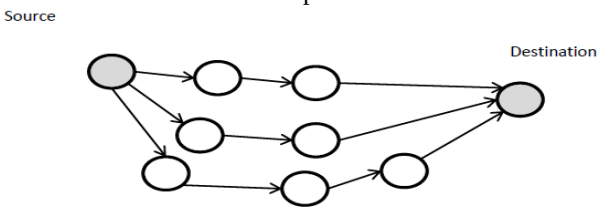
SPREAD

The basic idea of SPREAD (Security Protocol for reliable at a Delivery) [12] is to transform a secret message into multiple shares by secret sharing schemes and then deliver the shares via multiple independent paths to the destination so that even if a small number of nodes that are used to relay the message shares are compromised, the secret message as a whole in not compromised. Figure 4.5, shows SPREAD mechanism.

The node could make the final decision whether a message is delivered at certain time instant according to the security level and the availability of multiple paths. Also, the chosen set of multiple paths maybe changed from time to time to avoid any potential capture of those multiple paths. SPREAD is a mechanism to distribute the secrecy, first by secret sharing algorithm at the source node and then by multi-path routing while shares are delivered across the network, so that in the

https://dx.doi.org/10.22161/ijaers/3.12.46 *ISSN: 2349-6495(P) | 2456-1908(O)*

event that a small number of shares are compromised, the secret as a whole will not be compromised.



SPREAD Mechanism

SPREAD considers the security when massages are transmitted across the network, assuming the source and destination are trusted. SPREAD, scheme cannot address the confidentiality alone. It only statistically enhances such service. For example, it is still possible for adversaries to compromise all the shares, e.g. by collusion.

III. CONCLUSION

In this paper different secure versions of AODV, DSR and TORA protocols have also been reviewed. Traditionally, a secure ad hoc network has to meet different security requirements, Confidentiality, Integrity, Availability, Authentication and nonrepudiation. Different digital attacks have been developed to undermine the security of mobile Ad hoc networks.

ARIADNE provides point-to-point authentication of a routing message using a message authentication code (MAC) and a shared key between the two parties. ARIADNE copes with attacks performed by malicious nodes that modify and fabricate routing information, with attacks using impersonation and, in an advanced version, with the wormhole attack.

CONFIDANT is an on demand routing protocol designed for detecting and isolating misbehaving node. It maintains a global reputation value that leads to several issues like hiding bad behavior node. Distributed nature of mechanism leads to several inconsistencies in reputation value.

CORE is based on watchdog mechanism that can detect misbehaving nodes at forwarding level and not just the link level. A main problem with the watchdog approach is the vulnerability to blackmail attacks.

In SAODV, ownership of certified public keys enables intermediate enable intermediate nodes to authenticate all in-transit routing packets. The SAODV can be used to protect the route discovery mechanism of the AODV by providing security features like integrity, authentication and non-repudiation.

The ARAN protocol protects against exploits using modification, fabrication and impersonation. It uses asymmetric cryptography makes it a very costly protocol to use in terms of CPU and energy usage. It is also not immune to the wormhole attack.

SAR uses security information to dynamically control the choice of routes installed in the routing table. SAR will find the optimal route if all the nodes on the shortest path satisfy the security requirements. SAR may fail to find the route if the ad hoc network does not have a path on which all nodes on the path satisfy the security requirements in spite of being connected.

SPREAD provides security only when message are transmitted across the network. It assumes that the source and destination are trusted. It only enhances services such as confidentiality. These secure routing protocols provide many approaches to secure the MANETs, however there are still many open challenges remain unsolved because some of the secure routing protocols are designed by considering some certain known attacks but when an unknown attack is encountered, these protocols may collapse. Another reason may be due to achieving higher security always leads to more computation on each mobile node. In MANETs environment, resources are very limited, thus there will always be a trade between more security and more performance.

REFERENCES

[1] C. Siva Ram Murthy, B.S. Manoj, ―Ad Hoc Wireless Networks : Architectures and Protocols‖, Prentice Hall Publishers, May 2004, ISBN 013147023X.

[2] Yih-Chun Hu, Adrian Perrig, David B. Johnson. "Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks" MobiCom 2002, September 23-28, 2002, Atlanta, Georgia, USA.

[3] Perrig, R. Canetti, D. Tygar, and D. Song, "The TESLA Broadcast Authentication Protocol," Cryptobytes,, Volume 5, No. 2 (RSA Laboratories, Summer/Fall 2002), pp. 2-13.

[4] S. Buchegger and J. L. Boudec, ―Performance Analysis of the CONFIDANT Protocol Cooperation Of Nodes-Fairness In Dynamic Ad-hocNetworks,‖ Proc. IEEE/ACM Symp. Mobile Ad Hoc Networking and Computing (MobiHOC), 2002.

[5] Y. KO and N. H.Vaidya, ―Location-Aided Routing (LAR) in Mobile AHoc Networks,‖ Proc. ACM MOBICOM 1998, Oct. 1998, pp. 66–75.

[6] D. A. Maltz, ―Resource Management in Multi-hop Ad Hoc Networks,‖CMU School of Computer Science Technical Report CMU-CS-00-150,Nov. 21, 1999.

[7] Y. Hu and D. B. Johonson, ―Securing Quality-of-Service Route Discoveryin On-Demand Routing for Ad Hoc Networks,‖ Proc. ACM SASN_04, Oct. 20, 2004.

[8] Y. Hu and A. Perrig, ―A Survey of Secure Wireless Ad Hoc Routing,‖IEEE Computer Society, 2004.

[9] D. A. Maltz, ―Resource Management in Multi-hop Ad Hoc Networks,‖CMU School of Computer Science Technical Report CMU-CS-00-150,Nov. 21, 1999.

[10] KimayaSanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields and Elizabeth M. Belding royer. "A Secure Routing Protocol for Ad Hoc Networks" (ARAN) In

https://dx.doi.org/10.22161/ijaers/3.12.46 *ISSN: 2349-6495(P) | 2456-1908(O)*

International Conference on Network Protocols (ICNP), Paris, France, November 2002.

[11] Y. Wang, G. Attebury, and B. Ramamurthy, ―A Survey of SecurityIssues in Wireless Sensor Networks,‖ IEEE Commun. Surveys &Tutorials,vol. 8, no. 2, Apr. 2006.

[12] L. Lilien, ―Developing Pervasive Trust Paradiam for Authentication andAuthorization,‖ Cracow Grid Wksp. (CGW‘03), Cracow, Poland, Oct.2003.

[13] Neeraj Arora, Dr. N.C. Barwar, "Performance Analysis of DSDV, AODV and ZRP under Black hole attack", International Journal of Engineering Research & Technology (IJERT), Volume 3, Issue 04, April 2014.

[14] Neeraj Arora and Dr. N.C. Barwar , (2014) , "Evaluation of AODV , OLSR and ZRP Routing Protocols under Black hole attack" , International journal of Application in Engineering & Management , Volume 3 , Issue 4 ,pp. 2319 4847