IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 8, October 2014.
www.ijiset.com
ISSN 2348 – 7968

Routing Protocols towards Security objective of Mobile Adhoc Networks – A Survey

S. Sutha , Dr. B. Anandhi
Asst.Professor in Department of MCA, SSM college of Engineering Komarapalayam,Tamilnadu,India
Asst.Professor & Head in Computer Science (UG & PG), Vellalar College for Women Erode, Tamilnadu, India.

Abstract

A Mobile Ad-hoc Network (MANET) is form over wireless media by the various mobile nodes. In MANET communication between two mobile devices are performed by routing protocol, in which each mobile node can directly communicate with other mobile node if both mobile nodes are within transmission range. Otherwise the nodes present in between have to forward the packets for them on network. The strength of its infrastructure (wireless nature) also becomes the point of its greatest vulnerability. Thus decreasing the confidence level of the system as it pertains to availability, reliability, data integrity and privacy concerns. In this paper we try to explore basics of routing protocols and possible attacks. Routing protocol can employed encryption of data transmission, physical security of networks and protection against attacks. We will also investigate a number of wireless network attacks, examining the methodology behind such attacks as well as exploring preventive measures that may be taken for secure data transmission.

Keywords:, *Key management, MANET, routing attacks, security, unicast routing protocol.*

1. Introduction

An Ad-Hoc network is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies allowing people and devices to internet work without any preexisting communication infrastructure. Security is a critical issue in MANET because the primary applications of adhoc networks are the military applications, such as the tactical communications in a battlefield, where the environment is hostile and the operation is security-sensitive. While MANETs bring many attractive features for future network communications they also introduce many challenges related to (Taneja & Kush, 2010):

- unicast routing
- multicast routing
- dynamic network topology
- speed
- frequency of updates or network overhead
- scalability
- mobile agent based routing
- Quality of Service (QoS)
- energy efficient/power aware routing
- secure routing

2. Unicast Routing Protocols

Routing is the process to moving information / packet from a source node to a destination node in a mobile ad-hoc network. During routing process, at least one intermediate node within the network is encountered [4].

Routing protocol in Mobile ad-hoc network is divided into following types:

1) Unicast Routing Protocol
2) Multicast Routing Protocol
3) Broadcast Routing Protocol.

In this survey paper we will discuss only Unicast routing protocols. Fig 2.1. Classification of various unicast routing protocol in MANET

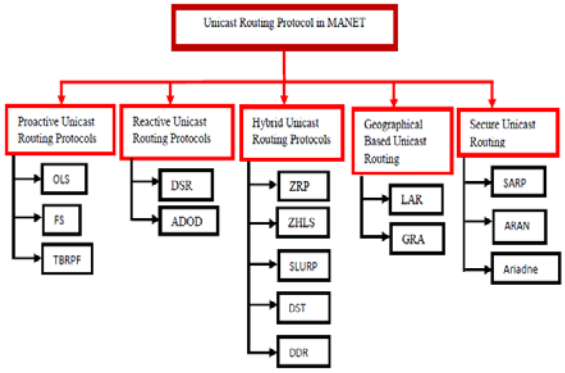

Fig 2.1. Classification of various unicast routing protocols

2.1. Unicast Routing Protocol

In MANET most of applications are base on Unicast communication. In Unicast source mobile node transmit data packet to destination. While forwarding data packet dispatch node use the destination address in the data packet to look it up in routing table. If the destination address found in routing table the data packet will send to the corresponding next hop. But in such condition every

ISSN 2348 – 7968

node maintains the routing table in network. So the problem is that how the routing table is created and maintained in MANET. Unicast routing protocols are further divided into two categories:

2.1.1. Proactive Unicast Routing Protocol

In Proactive Unicast routing protocol each node in MANET maintains routing information to every other node in network to compute shortest path from the source to every destination node, which consumes lots of bandwidth. Such routing information is kept in many different types of tables. Such tables are time to time updates if network topology changes or a node moves from network. Proactive unicast routing protocol are Divided as Optimized Link State Routing Protocol (OLSR), Fishey State Routing Protocol (FSR) and Topology Broadcast Based on Reverse Path Forwarding Routing Protocol (TBRPF).

Optimized Link State Routing Protocol: OLSR **[17]** main aim is for large and dense Mobile Ad-Hoc Network. OLSR works on Multipoint Relaying flooding techniques to reduced topology broadcast packets. OLSR works according to the following points.

- Every mobile node broadcast **"hello"** message periodically to its neighbor. With this hello message every mobile node can obtain topological information for every node in MANET.
- Now based on topological Information, A node will select a subset of its neighbor to act as multipoint relaying nodes.
- Every node contains its global topological information and update, shortest path from source node to every other node can computed with dijkstra's Algorithm.

Fishey State Routing Protocol: FSR was proposed in **[18]** for aim at large scale and wit high mobility MANET. Name of this protocol comes from property of eye's fish. Fishey State Routing Algorithm works on following method.

- Based on distances the network is divided into different scopes. For example if the nodes are in 3 hops distance, they will come in same scope. Other node will come outer scope.
- The nodes which are in different scope, Routing entries corresponding to these nodes are sent at different frequencies and routing entries for inner nodes are sent at highest frequency and other entries are sent at lower frequency. Because of this reason the nearby node will receive more up to date link state updates compare to the node far away node.

Topology Broadcast Based on Reverse Path Forwarding Routing Protocol: TBRPF was proposed for several hundred of mobile nodes or high mobility in MANET **[19].** In TBRPF each mobile node in network keeps incomplete global topological information. To reduce routing overhead TBRPF adopts following optimization steps:

- hello‖ messages are exchanged among neighboring nodes periodic and differential. Only the changes of neighbor status are included in ―hello‖ message.
- A part of spanning tree is broadcast to its neighbors if mobile node _*A*_ finds itself is on the path from its neighbor _*B"* to a destination _*C"* in the *„A"* rooted spanning tree, it will put node *„C"* and its adjacent links in the reportable topology sent to neighbors.
- Whenever required like network topology updated, mobile node mobility etc, it will update with *"hello"* message.

TABLE I
COMPARISON BETWEEN OLSR, FSR & TBRPE

Protocol	RS	CT	MO	CO
OLSR	F	O(D.I)	$O(N^2)$	$O(N^2)$
FSR	F	O(D.I)	$O(N^2)$	O(N)
TBRPE	F	O(D) or D+2 for link failure	$O(N^2)$+ O(N)+ O(N+V)	$O(N^2)$

RS=> Route Structure, CT=> Convergence time, MO=:Memory overhead, CO=> Control Overhead, V=>Number of neighboring nodes, D=>Diameter of the network, N=> Number of nodes in the network

2.1.2 Reactive Unicast Routing Protocol

Reactive protocols are also known as On demand routing protocol. Such protocol were reduced the overheads of proactive protocol by maintaining route information for active routes. Its mean the routing information is required and maintained only when one node wants to send data packet to destination.

In reactive routing protocol the overall routing process is divided into following steps.

a) *Route Discovery Process:* In route discovery process of MANET, if source node does not have route information in its routing table, source node

ISSN 2348 – 7968

broadcast a route discovery packet to the MANET to find out route between source and destination.

b) *Routing Maintenance:* once the route between source and destination has been setup.

Reactive unicast routing protocol are Divided as Dynamic Source Routing Protocol (DSR) and Ad-hoc On-Demand Distance Vector Routing Protocol (AODV).

Dynamic Source Routing Protocol: In DSR **[20]** each packet required to carry the full address from source to destination. This property of DSR shows that it is not very effective protocol for large MANET because of the overhead carried out by packet will increase as network size increase. This is the only reason that DSR consume high bandwidth. DSR performed better for small network size.

Ad-hoc On-Demand Distance Vector Routing Protocol: AODV **[21]** is based on DSR and DSDV routing protocol. It uses periodic sequence numbering procedure of DSDV and route discovery as DSR. In AODV the source data packet contains destination address to reduced routing overhead.AODV adaptable to highly dynamic networks.

TABLE II
COMPARISON BETWEEN DSR & AODV

Protocol	RS	MR	TC(RD)	TC(RM)	CC(RD)	CC(RM)
DSR	F	Yes	O(2D)	O(2D)	O(2N)	O(2N)
AODV	F	No	O(2D)	O(2D)	O(2N)	O(2N)

RS=> Route Structure, MH=> Multiple Routing, RD=: Route Discovery, RM=> Route Maintenance, RD=> Route Distance, CC=> Communication complexity, D=>Diameter of the network, N=> Number of nodes in the network

2.1.3. Hybrid Unicast Routing Protocols

Hybrid protocols are the protocol which combines the nature of both proactive routing protocol and s routing protocol. Hybrid protocols are known as new generation protocols. Hybrid protocol reduced route discovery overheads by allowing nodes with closeness to work together to from some short of a backbone. Hybrid protocols are proposed based on zone (region).Examples of hybrid routing protocols include Zone Routing Protocol (ZRP)[22], and zone based Hierarchical Link state Routing Protocol(ZHLS)[23].

2.1.4. Geographical Based Unicast Routing Protocol

Such routing algorithms are working on the geographical location of mobile nodes. Graphical location for a mobile node is identified by GPS. LAR and GAR are the protocol which came into the category of geographical based unicast routing protocol in MANETs.

2.1.5. Security Aware Routing Protocol

Security is very important constraint in MANET, because every data packet sent from source mobile node to destination should be kept secure during the routing process so that attackers cannot read the data packet before delivered to the destination.

3. Issues Releted To Routing In Mobile Adhoc Networks

3.1 Infrastructure

An Ad-hoc network is an infrastructure less network. Unlike traditional networks there is no pre-deployed infrastructure such as centrally administered routers or strict policy for supporting end-to-end routing. The nodes themselves are responsible for routing packets. Each node relies on the other nodes to route packets for them. Mobile nodes in direct radio range of one another can communicate directly, but nodes that are too far apart to communicate directly must depend on the intermediate nodes to route messages for them.

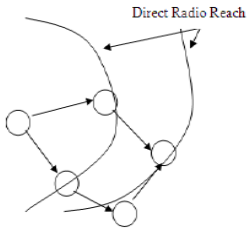

Fig 3.1.a. Routing in Adhoc networks

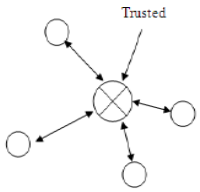

Fig 3.1.b Routing in traditional networks

3.2 Frequent changes in network topology

Ad-hoc networks contain nodes that may frequently change their locations. Hence the topology in these networks is highly dynamic. This results in frequently changing neighbors on whom a node relies for routing. As a result traditional routing protocols can no longer be used in such an environment. This mandates new routing protocols that can handle the dynamic topology by facilitating
fresh route discoveries.

3.3 Problems associated with wireless communication

As the communication is through wireless medium, it is possible for any intruder to tap the communication easily. Wireless channels offer poor protection and routing related control messages can be tampered. The wireless medium is susceptible to signal interference, jamming, eavesdropping and distortion. An intruder can easily eavesdrop to know sensitive routing information or jam the signals to

ISSN 2348 – 7968

prevent propagation of routing information or worse interrupt messages and distort them to manipulate routes. Routing protocols should be well adopted to handle such problems.

3.4 Problems with existing Ad-hoc routing protocols

3.4.1 Implicit trust relationship between neighbors

Current Ad-hoc routing protocols inherently trust all participants. Most Ad-hoc routing protocols are cooperative by nature and depend on neighboring nodes to route packets. This naive trust model allows malicious nodes to paralyze an Ad-hoc network by inserting erroneous routing updates, replaying old messages, changing routing updates or advertising incorrect routing information. While these attacks are possible in fixed network as well, the Ad-hoc environment magnifies this makes detection difficult.

3.4.2 Throughput

Ad-hoc networks maximize total network throughput by using all available nodes for routing and forwarding. However a node may misbehave by agreeing to forward packets and then failing to do so, because it is overloaded, selfish, malicious or broken. Misbehaving nodes can be a significant problem. Although the average loss in throughput due to misbehaving nodes is not too high, in the worst case it is very high.

3.4.3 Attacks using modification of protocol fields of messages

Current routing protocols assume that nodes not alter the protocol fields of messages passed among nodes. Routing protocol packets carry important control information that governs the behavior of data transmission in Ad-hoc networks. Since the level of trust in a traditional Adhoc network cannot be measured or enforced, enemy nodes or compromised nodes may participate directly in the route discovery and may intercept and filter routing protocol packets to disrupt communication. Malicious nodes can easily cause redirection of network traffic and DOS attacks by simply altering these fields.

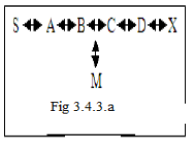

Fig 3.4.3.a

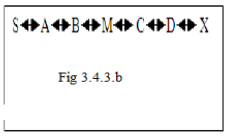

Fig 3.4.3.b

For example, in the network illustrated in Figure 3.4.3.a, b a malicious node M could keep traffic from reaching X by consistently advertising to B a shorter route to X than the route to X, which C is advertising.

4. Materials and Methods

In this study, we broadly classify the study into two sections namely, Attack in MANET and Intrusion Detection.

4.1. Attacks in MANET

Snooping where the nodes misuse the inherent trust between nodes to eavesdrop on packets to obtain packet payload data and routing information. Flood storm attacks where malicious nodes flood the network with route requests and route replies, effectively paralyzing the network. In tampering attacks, the intermediate nodes modify the packet content or change source and destination address. Data packets are prevented from reaching node and also nodes are prevented from sending data packets in denial of service attacks (Douligeris and itrokosta, 2004). In rushing attacks, a malicious node establishes routes through it (Hu *et al*., 2003b).

Malicious nodes advertise itself as having shortest route to destination node, thus all traffic is forwarded to it and the node does not forward any traffic at all in Blackhole attack. These black holes can be detected only by 4 monitoring for lost traffic (Weerasinghe andFu, 2007).

A wormhole attack (Hu *et al*., 2003a; 2005) creates a tunnel called, wormhole tunnel, between two nodes. A wormhole tunnel diverts packets to some random node in the network rather than the intended destination. The wormhole attack is shown in Fig. 3.4.3.a. The path W-W, in Fig. 3.4.3.a denotes the wormhole tunnel. The correct path is S-A-B-C-D.

A Sybil attack (Douceur, 2002) occurs when the Malicious node acts like two or more nodes. Sybil nodes are created by false identities or impersonation of nodes in the network.

4.2. Intrusion Detection Systems

Many researchers have conducted various studies on the Intrusion Detection Systems (IDS) for MANET. Some of them based on DSR and AODV are reviewed in the following paragraphs.

Tseng *et al*. (2003) proposed a solution using specification based technique to detect attacks on AODV. Specification based monitoring capture the correct behavior by comparing the behavior of objects with their associated security specifications. Thus,intrusions which cause incorrect behavior can be detected without exact knowledge about them. The proposed approach uses finite state machines for describing the valid flow of AODV routing behavior. Violations in the specifications are detected by the distributed network monitors. The approach also

ISSN 2348 – 7968

proposes to add a field in the protocol message to enable monitoring. The proposed algorithm is based on tree structure and a node coloring scheme. The IDS is built on the monitoring architecture that traces AODV request-reply flow. Detail procedures for constructing and processing the trees for detecting attacks are discussed. The proposed method detects AODV routing attacks efficiently and with low overhead.

Zapata (2002) presented AODVSTAT, a etworkbased, real time IDS for networks based on AODV. The study also surveys various attacks against AODV based network and is summarized as shown in **Fig. 2.**

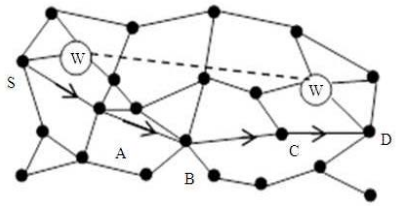

Fig.4.a. Wormhole attack

The proposed tool (Vigna *et al*., 2004) is based on the State Transition Analysis Technique (STAT). AODVSTAT sensors are deployed either on stand alone or distributed basis on a subset of the nodes of the network. The sensors perform real-time state ful analysis on the packet stream to detect signs of intrusions. Experimental results show that the proposed method successfully detects attacks against AODV routing protocol with low number of false positives and low overhead.

Marti *et al*. (2000) proposed a watchdog mechanism implemented on DSR by categorizing nodes based on dynamic measured behavior. The proposed method complemented DSR with a watchdog and pathrater. The watchdog was used for detection of malicious behavior and runs on each node, listening to all the transmissions of neighboring node. Pathrater is used for trust management and routing policy, every used path is rated. A buffer is maintained by the watchdog which contains recently sent packets and it is removed fromthe buffer when the packet is forwarded by the next hop. If the packet remains in the buffer, watchdog assumes that the node is misbehaving. Thus, enabling nodes to avoid malicious nodes in their routes and deliver the data packet. On simulation, the proposed method performed efficiently, increasing the throughput by 17% in the presence of 40% misbehaving nodes.

Mangai and Tamilarasi (2011) studied the malicious nodes in Improved Location aided Cluster based Routing Protocol (ILCRP) for GPS enabled MANETs. The proposed method used the location information with security against attacks in high packet delivery ratio. Simulations are performed using NS2 by varying the number of nodes. The simulation results show that the ILCRP provides higher delivery ratio with IDS.

It is observed that watchdog mechanism (Marti *et al*., 2000) is not only able to mitigate attacks but also improve the throughput with high number of misbehaving nodes. Though Tseng *et al*. (2003) technique displays the type of attacks better than other methods found in literature, it does not provide a mechanism to mitigate the attacks.

AODVSTAT, a network based,[1] real time IDS for networks based on AODV. The study also surveys various attacks against AODV based network and is summarized as shown in Fig.4.2.a.

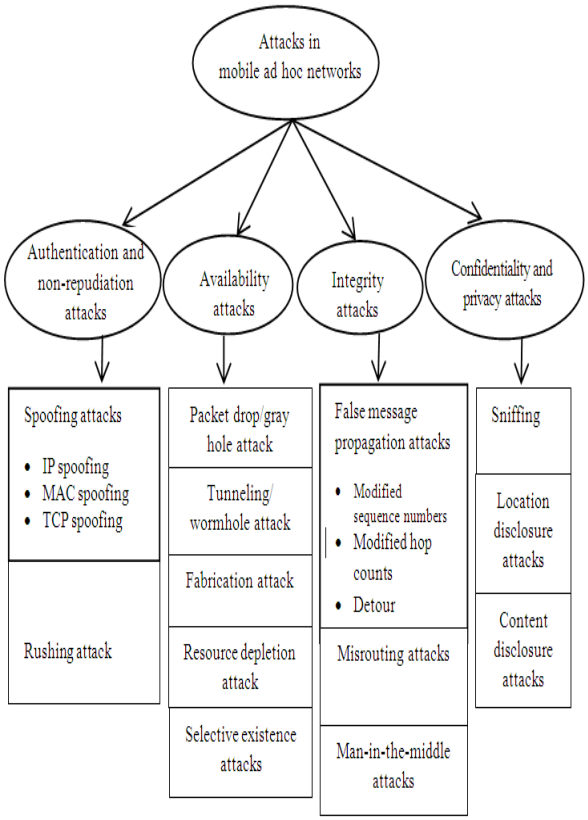

Fig .4.2.a various attacks in Mannet

5. Security objectives

5.1. Network Availability

[16] Availability is a key concern in wireless network security. It relates to the survivability and operability of a wireless network.

ISSN 2348 – 7968

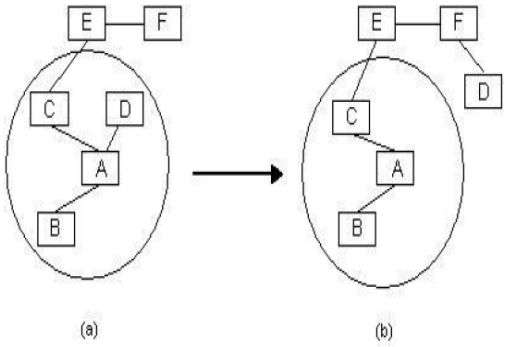

Fig.5.Changing Network Topology (Source[11]

5.1.1. Node Failure and Topological Changes.

In the event that nodes become inoperable the network must be able to provide redundancy that will allow it to continue functioning. The network must also be able to adjust when there is a change in the network topology. Availability ensures not only operational efficiency, but also data delivery. This is usually done by the routing protocol. (Fig. 5).

5.2. Denial of Service Attacks

A denial of service attack is the most common attack to deny network availability. There is the frame level attack and the physical level (RF) attack. Using algorithms and network configuration management tools, a frame-level attack may be prevented. (Needless to say, this requires more resources.) Although there are numerous scenarios for a physical (RF) DoS attack, the logistics is primarily the same.

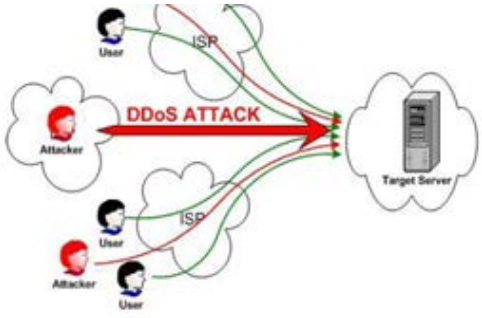

Figure 5.2.a. Denial of Service Attack (Source:[http://fedoraboost.blogspot.com/2010/12/linux-and-denial-of-service-dos.html])

Wireless devices use CSMA/CA (carrier sense multiple access with collision avoidance) protocol to transmit data between nodes. A node wishing to transmit data must first listen to the channel to check for activity. If the channel is idle, the node can begin transmission. Otherwise, the node must wait (back off) until the channel is free. By design most wireless devices share the communication medium. However, it is possible for a device to constantly transmit energy on the frequency (or operating bandwidth) of a wireless network, making the channel unavailable. This effectively denies all service (data transmission) on the network. (Figure 5.2.a) There is no realistic protection against such an attack. If a node has the appropriate hardware, a DoS attacked can be mitigated.

5.3. Data Integrity

Due to the nature and physical structure of wireless ad hoc networks, there is an increased risk of data corruption, whether intended or unintended. Techniques have already been noted that will lessen the possibility of intended data propagating through the system. Thus, it remains to be addressed how that accurate data can be assured.

5.4. Checksum

Wireless networks may use checksum algorithms for data verification. Based on the information in the stored in the data packet, a checksum (fixed-sized data) value is generated and transmitted along with the packet. The receiving node then computes the checksum of the information received and compares it the received checksum. Only verified data is further transmitted. Checksum algorithms can be as simple as bit parity or modular sum. As always, the complexity of the algorithm must be limited by the resources of the processing nodes.

5.5. Hash Function

A hash function is similar to checksum in that it can convert large, variably-sized data into a small data (hash value).

5.6. Non-repudiation

While this type of security may not be necessary in many wireless ad hoc networks, non-repudiation offers additional confidence in data integrity. It ensures that the originator (source node) of a message cannot deny having sent it and the receiver (receiving node) cannot deny having received the message. In the event a corrupted message is received from a node, that sending node can be flagged and its identity sent to other nodes to ignore its messages.

ISSN 2348 – 7968

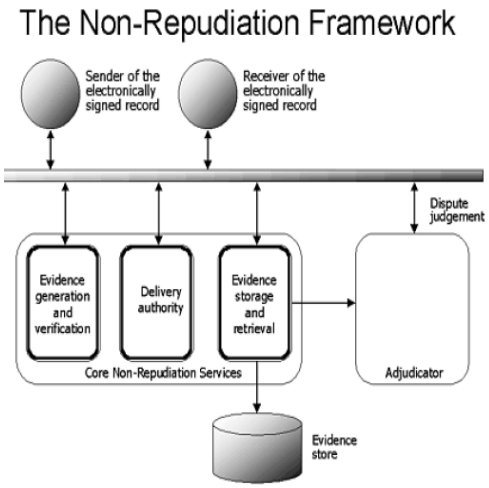

Fig 5.6. Modified from: Orfali,Robert,Harkey,Dan,& Jeri Edwards Client-Server Survival Guide. John Wiley & Sons: New York, 1999, p. 144. (Source: [http://www.archives.gov/records-mgmt/policy/electronic-signature-technology.html])

5.7. Access Security

As stated earlier, an inherent security flaw in a wireless network is its medium of communication. If the frequency of the communication channel is known, data packets can be read by an unauthorized node/device. For this reason, most wireless access points have a MAC (medium access control) ID filter. The administrator is able to permit or restrict access to devices with specific MAC IDs.

5.7.1. Mandatory Access Control (MAC)

MAC is primarily used by the government and is one of the strictest levels of control. It is a hierarchical approach to accessing resources. Access to all resources is defined by a system administrator. The user is unable to change the access control of a resource. All resource objects have labels, consisting of a classification and a category. Each user account also has a classification and category as it relates to a resource object. When a user tries to access a resource object, the classification and category of the user against the resource label is checked. Although MAC is the most secure access control environment, it imposes a high system management overhead.

5.7.2. Discretionary Access Control (DAC)

DAC allows the user to control access to their own data resources. This is generally seen in desktop operating systems. Each resource object has an associated access control list containing a list of authorized users and groups. Also, system administrators can grant permission to other users to resources. DAC is flexible, but also opens a security risk to the unintended granting of access to unauthorized users.

5.7.3. Role-based Access Control (RBAC)

RBAC is known as non-discretionary access control. Access to resource objects are based upon the user's role or function in the network system. Users may have multiple roles in the same system. A user, however, cannot be granted specific access to resources other than that which pertains to their role.

5.7.4. Rule-based Access Control (RBAC)

As implied by the name, access to resource objects is based on a set of predefined rules established by a system administrator. It also has an Access Control List associated with each resource. When access is attempted, the operating system checks the rules in the ACL list for that resource object.

5.8. Key Management System

A key management system in a wireless ad hoc network should provide security, robustness and scalability. An efficient KMS have the ability to quickly form keys, disallow the distribution and exposure if key material to unauthorized nodes, provide security against compromised nodes, allow key updates, and revoke keys from compromised nodes. [16] The KMS should also operate efficiently under increasing network size and node density. (Fig.5.8) Signed routing information is a one-to-many signing and verification security methodology. Messages that have been broadcasted too many nodes are subject to verification and validation by the receivers. There may be exceptions to such validation procedures in neighbor-detection and network topology discovery.

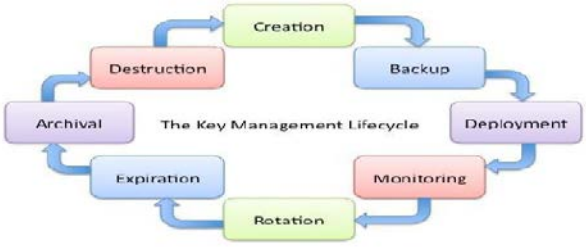

Fig 5. 8. Key Management Systems (Source:[http://www.secureconsulting.net/2008/03/the_key_management_lifecycle_1.html])

The key management system may be classified as contributory or distributive. In the contributory key management system every node participates in the key management. Distributive key management systems each key originates from each node. That key is distributed to other nodes. Distributive systems involve a trusted third party

ISSN 2348 – 7968

public key system and/or symmetric systems. (See Fig.5 The traditional certification authority is employed using an identity based scheme. Hence, the difference in the contributory and distributive system scheme is the contributive system lacks a trusted third party that is responsible for generating and distributing keys.

6. Conclusion

This study investigated various types of Routing protocols, possible attacks in a MANET. Various types of attacks and solution/responses have been declared. That is to say, some key issues were highlighted that are imperative to the availability, security and robustness of wireless network. Access Mechanism, Data Integrity and Key management systems are seen as an emerging method of security objectives wireless networks. Finally we have to further explore deep into the various method of providing basics knowledge about Adhoc Routing Protocols and attacks.

References

[1] Zapata, M.G., 2002. Secure ad hoc on-demand distance vector routing. *ACM Mobile Comput. Commun. Rev., 6: 106-107. DOI: 10.1145/581291.581312.*

[2] Douligeris, C. and A. Mitrokosta, 2004. DDoS attacks and defense mechanisms: Classification and stateof- the-art. *Comput. Netw., 44: 643-666. DOI:10.1016/j.comnet.2003.10.003*

[3] Hu, Y.C., A. Perrig and D.B. Johnson, 2003b. Rushing attacks and defense in wireless ad hoc network routing protocols. *Proceedings of the 2nd ACM Workshop on Wireless Security, Sept. 19-19,* ACM Press, San Diego, CA, USA., pp: 30-40. DOI: 10.1145/941311.941317

[4] Mehran Abolhasan, Tadeusz Wysocki, and Eryk Dutkiewicz. A review of routing protocols for mobile ad hoc networks. Technical report, *Telecommunication and Information Research Institute, University of Wollongong, Wollongong, NSW 2522; Motorola Australia Research Centre, 12 Lord St., Botany, NSW 2525, Australia, 2003.*

[5] Jean-Pierre Hubaux,Levente Buttyyan,Srdan Capkun, *The Quest for Security inMobile Ad-hoc Networks* .

[6] Weerasinghe, H. and H. Fu, 2007. Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation. *Future Generat. Commun. Netw., 2: 362- 367. DOI: 10.1109/FGCN.2007.184*

[7] Douceur, J.R., 2002. The sybil attack. Peer-to-Peer Syst. *Lecture Notes Comput. Sci., 2429: 251-260. DOI: 10.1007/3-540-45748-8_24*

[8] Hu, Y.C., A. Perrig and D.B. Johnson, 2003a. Packet leashes: *A defense against wormhole attacks in wireless networks.* Proceedings of the IEEE Societies 22nd Annual Joint Conference of the IEEE Computer and Communications, Mar. 30-Apr. 3, IEEE Xplore Press, pp: 1976-1986. DOI: 10.1109/INFCOM.2003.1209219.

[9] Hu, Y.C., A. Perrig, D.B. Johnson, 2005. Ariadne: A secure on-demand routing protocol for ad hoc networks. *J. Wireless Netw., 11: 21-38. DOI:10.1007/s11276-004-4744-y.*

[10] Tseng, C.Y., P. Balasubramanyam, C. Ko, R. Limprasittiporn and J. Rowe *et al*., 2003. A specification-based intrusion detection system for AODV. *Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks,* Oct. 27- 30, ACM Press, Washington, DC, USA., pp: 125- 134. DOI: 10.1145/986858.986876

[11] Y.C. Hu, A. Perrig,"A Survey of Secure Wireless Ad Hoc Routing", *IEEE Security and Privacy, Vol. 2, No. 3, pp. 28-39, 2004.*

[12] Mangai, S. and A. Tamilarasi, 2011. An improved location aided cluster based routing protocol with intrusion detection system in mobile ad hoc networks. *J. Comput. Sci., 7: 505-511. DOI:10.3844/jcssp.2011.505.511*

[13] Marti, S., T.J. Giuli, K. Lai and M. Baker, 2000. Mitigating routing misbehavior in mobile ad hoc networks. *Proceedings of the 6th Annual nternational Conference on Mobile Computing and Networking,* Aug. 06-11, ACM Press, Boston, Massachusetts, U.S., pp: 255-265. DOI:10.1145/345910.345955

[14] Tseng, C.Y., P. Balasubramanyam, C. Ko, R. Limprasittiporn and J. Rowe *et al*., 2003. A specification-based intrusion detection system for AODV. *Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks,* Oct. 27- 30, ACM Press, Washington, DC, USA., pp: 125- 134. DOI: 10.1145/986858.986876

[15] Vigna, G., S. Gwalani, K. Srinivasan, E.M. Belding- Royer and R.A. Kemmerer, 2004. An intrusion detection tool for AODV-based ad hoc wireless networks. *Proceedings of the 20th Annual Computer Security Applications Conference,* Dec. 6-10, IEEE Xplore Press, pp: 16-27. DOI: 10.1109/CSAC.2004.6

[16] Cayirci, E. and Rong, *C. Security in Wireless Ad Hoc and Sensor Networks.* John Wiley and Sons. Chichester, West Sussex, United Kingdom. 2009.

[17] Amir Qayyum, Laurent Viennot, and Anis Laouiti, ―Optmized Link State Routing Protocol, *draft-ieft-manet-olsr-06.txt, September 2002(expired).*

[18] Mario Gerla, Ziaoyan Hong, and Guangyu Pei, ―Fisheye State Routing Protocol (FSR) for Ad Hoc Networks‖, *draft-ietf—manet-fsr-03.txt, June 2002(Work in progress).*

[19] Richard G. Ogier, Fred L. Templin, Bhargav Bellur, and Mark G. Lewis, ―Topology Broadcast Based on Reverse-Path Forwading (TBRPF)‖, *draft-ietf-manet-tbrpf-05.txt, March 2002.*

[20] M. S. Corson, A. Ephremider, A Distributed routing algorithm for mobile wireless networks, *ACM/Baltzer Wireless Networks 1(1)(1995) 61-81.*

[21] S. Das, C. Perkins, E. Royer, Ad hoc on demand distance vector (ADOCV) routing , *Internet Draft, draft-ietf-manet-adov-11.txt, work in progress, 2002.*

[22] Z. J. Hass, R. Pearlman, Zone routing protocol for ad-hoc networks, *Internet Draft, draft-ietf-manet-zrp-02.txt, work in progress, 1999.*

[23] M. Joa-Ng, I.-TLu, A peer-to-peer zone based tow-level link state routing for mobile ad hoc networks, *IEEE Journal on Selected Areas in Communications 17(8) (1999) 1415-1425.*