IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 02, Aug 2011
ISSN (Online): 2231-5268
www.ijcsms.com

A Survey on Security Issues in Mobile Ad-hoc Networks

Sonia Boora[1], Yogesh Kumar[2], Bhawna Kochar

[1]Asst. Professor, RIMT, Chidana
soniyaboora11@yahoo.co.in,
[2]Lecturer, HIT, Asouda
sangwan130@gmail.com
[3]M.Tech. Scholar , P.D.M.C.E.,Bahadurgarh
bhawna.kochhar9@gmail.com

ABSTRACT

Current technologies and security advances have made networks systems and applications very popular and widely used. The pervasive and practical aspects of wireless Mobile Ad Hoc Networks (MANET) made them very popular as well. this created the need for securing MANET's to provide users with authentic communications, Secure, and robust information exchange and efficient security mechanisms .however , many of the security solutions devised for regular networks are not as efficient nor as effective on MANET's. This paper investigates the security issues of MANET's as well as survey some available techniques to secure it.

Keywords: *MANET, Multihop, Adhoc Networks, Topologies.*

I INTRODUCTION

With recent performance advancements in computer and wireless communications technologies, advanced mobile wireless computing is expected to see increasingly widespread use and application, much of which will involve the use of the Internet Protocol (IP) suite. The vision of mobile ad hoc networking is to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes.
Such networks are envisioned to have dynamic, sometimes rapidly-changing, random, multihop topologies which are likely composed of relatively bandwidth constrained wireless links.

A.) Challenges in Ad hoc

The technology of Mobile Ad hoc Networking is somewhat synonymous with Mobile Packet Radio Networking (a term coined via during early military research in the 70's and 80's), Mobile Mesh Networking (a term that appeared in an article in The Economist regarding the structure of future military networks) and Mobile, Multihop, Wireless Networking (perhaps the most accurate term, although a bit cumbersome). There is current and future need for dynamic ad hoc networking technology. The emerging field of mobile and nomadic computing, with its current emphasis on mobile IP operation, should gradually broaden and require highly-adaptive mobile networking technology to effectively manage multihop, ad hoc network clusters which can operate autonomously or, more than likely, be attached at some point(s) to the fixed Internet. MANET can be established extremely flexibly without any fixed base station in battlefields, military applications, and other emergency and disaster situation. Some applications of MANET technology could include industrial and commercial applications involving cooperative mobile data exchange.

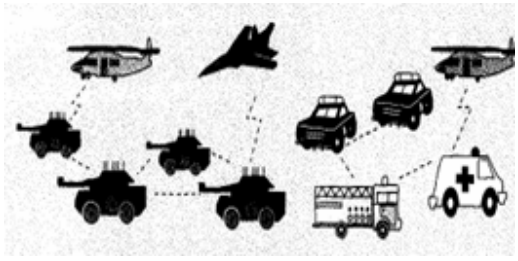

Figure 1 Example Applications of manets

In addition, mesh-based mobile networks can be operated as robust, inexpensive alternatives or enhancements to cell-based mobile network infrastructures. There are also existing and future military networking requirements for robust, IP-compliant data services within mobile wireless communication networks many of these networks consist of highly-dynamic autonomous topology segments.
Also, the developing technologies of "wearable" computing and communications may provide

applications for MANET technology. When properly combined with satellite-based information delivery, MANET technology can provide an extremely flexible method for establishing communications for fire/safety/rescue operations or other scenarios requiring rapidly-deployable communications IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009 242 with survivable, efficient dynamic networking. There are likely other applications for MANET technology which
are not presently realized or envisioned by the authors. It is, simply put, improved IP-based networking technology for dynamic, autonomous wireless networks.

B.) Characteristics of MANETs

A MANET consists of mobile platforms (e.g., a router with multiple hosts and wireless communications devices)--herein simply referred to as "nodes"--which are free to move about arbitrarily. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices, and there may be multiple hosts per router. A MANET is an autonomous system of mobile nodes. The system may operate in isolation, or may have gateways to and interface with a fixed network.
In the latter operational mode, it is typically envisioned to operate as a "stub" network connecting to a fixed internet work. Stub networks carry traffic originating at and/or destined for internal nodes, but do not permit exogenous traffic to "transit" through the stub network.
MANET nodes are equipped with wireless transmitters and receivers using antennas which may be omni directional (broadcast), highly- directional (point-to-point), possibly steer able, or some combination thereof. At a given point in time, depending on the nodes' positions and their transmitter and receiver coverage patterns, transmission power levels and co-channel interference levels, a wireless connectivity in the form of a random, multihop graph or "ad hoc" network exists between the nodes. This ad hoc topology may change with time as the nodes move or adjust their transmission and reception parameters.

MANETs have several salient characteristics:

1) Dynamic topologies: Nodes are free to move arbitrarily; thus, the network topology--which is typically multihop--may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links.

2) Bandwidth-constrained, variable capacity links: Wireless links will continue to have significantly lower capacity than their hardwired counterparts. In addition, the realized throughput of wireless communication after accounting for the effects of multiple access, fading, noise, and interference conditions etc.--is often much less than a radio's maximum transmission rate. One effect of the relatively low to moderate link capacities is that congestion is typically the norm rather than the exception, i.e. aggregate application demand will likely approach or exceed network capacity frequently. As the mobile network is often simply an extension of the fixed network infrastructure, mobile ad hoc users will demand similar services. These demands will continue to increase as multimedia computing and collaborative networking applications rise.

3) Energy-constrained operation: Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design criteria for optimization may be energy conservation.

4) Limited physical security: Mobile wireless networks are generally more prone to physical security threats than are fixed- cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered. Existing link security techniques are often applied within wireless networks to reduce security threats. As a benefit, the decentralized nature of network control in MANETs provides additional robustness against the single points of failure of more centralized approaches.

C.) Security objectives

The preliminary security goals can be considered as an extension of the objectives for traditional Networks.Two mnemonics, ‘CIA’ (Confidentiality, Integrity, Availability) and ‘Triple A’ (Authentication, Authorization, Accounting) are generally used as the criteria for a secure network. These attributes must be satisfied, as well as some other factors like privacy, physical security etc. must be considered due to the pervasive nature of MANET.

Confidentiality - The information must not reach

others, who are not entitled to receive the information. Not only data, routing information must also remain secure.

Integrity - One shouldn't be able to modify the data during transit. Both malicious attacks and benign failure, such as radio propagation impairment could cause information corruption.

Availability - The network can still operate when faced with a DoS attack. These types of attacks can be launched at any layer of the network causing physical jamming, disconnection, and malfunction of key management service and routing protocol.

Authentication - The receiver should be able to identify the sender correctly. No other person can disguise as the sender.

Non-repudiation - The sender can't falsely deny later that he has sent a message. This is useful for detection and isolation of compromised nodes.
Access control - Information is being handled by authorized nodes.

Authorization - Rules and regulations that define restriction of responsibilities of network and individual nodes.

In addition to this, Trustworthiness can be considered as another dimension that deals with privacy, correctness, reliability, and fault-tolerance.

II VULNERABILITIES OF THE MOBILE AD HOC NETWORKS

Because mobile ad hoc networks have far more vulnerabilities than the traditional wired networks, security is much more difficult to maintain in the mobile ad hoc network than in the wired network. In this section, we discuss the various vulnerabilities that exist in the mobile ad hoc networks.

A.) Lack of Secure *Boundaries*

The meaning of this vulnerability is self-evident: there is not such a clear secure *boundary* in the mobile ad hoc network, which can be compared with the clear line of defense in the traditional wired network. This vulnerability originates from the nature of the mobile ad hoc network: freedom to join, leave and move inside the network.
In the wired network, adversaries must get physical access to the network medium, or even pass through several lines of defense such as firewall and gateway before they can perform malicious behavior to the targets [6]. However, in the mobile ad hoc network, there is no need for an adversary to gain the physical access to visit the network: once the adversary is in the radio range of any other nodes in the mobile ad hoc network, it can communicate with those nodes in its radio range and thus join the network automatically. As a result, the mobile ad hoc network does not provide the so-called secure boundary to protect the network from some potentially dangerous network accesses.

Lack of secure boundaries makes the mobile ad hoc network susceptible to the attacks. The mobile ad hoc network suffers from all-weather attacks, which can come from any node that is in the radio range of any node in the network, at any time, and target to any other node(s) in the network. To make matters worse, there are various link attacks that can jeopardize the mobile ad hoc network, which make it even harder for the nodes in the network to resist the attacks. The attacks mainly include passive eavesdropping, active interfering, and leakage of secret information, data tampering, message replay, message contamination, and denial of service.

B.) Threats from Compromised nodes Inside the Network

In the previous subsection, we mainly discuss the vulnerability that there is no clear secure boundaries in the mobile ad hoc network, which may cause the occurrences of various link attacks. These link attacks place their emphasis on the links between the nodes, and try to perform some malicious behaviors to make destruction to the links. However, there are some
other attacks that aim to gain the control over the nodes themselves by some unrighteous means and then use the compromised nodes to execute further malicious actions. This vulnerability can be viewed as the threats that come from the compromised nodes inside the network.
Since mobile nodes are autonomous units that can join or leave the network with freedom, it is hard for the nodes themselves to work out some effective policies to prevent the possible malicious behaviors from all the nodes it communicate with because of the behavioral diversity of different nodes. Furthermore, because of the mobility of the ad hoc network, a
compromised node can frequently change its attack target and perform malicious behavior to different node in the network, thus it is very difficult to track

the malicious behavior performed by a compromised node especially in a large scale ad hoc network. Therefore, threats from compromised nodes inside the network are far more dangerous than the attacks from outside the network, and these attacks are much harder to detect because they come from the compromised nodes, which behave well before they are compromised.

A good example of this kind of threats comes from the potential *Byzantine failures* encountered in the routing protocol for the mobile ad hoc network [4]. We call it a Byzantine failure when a set of nodes are compromised in such a way that the incorrect and malicious behavior cannot be directly detected because of the cooperation among these compromised nodes when they perform malicious behaviors. The compromised nodes may seemingly behave well; however, they may actually make use of the flaws and inconsistencies in the routing protocol to undetectably destroy the routing fabric of the network, generate and advertise new routing information that contains nonexistent link, provide fake link state information, or even flood other nodes with routing traffic. Because the compromised nodes cannot be easily recognized, their malicious behaviors are prone to be ignored by other nodes.

Therefore Byzantine failure is very harmful to the mobile ad hoc network.rom above we find that the threats from compromised nodes inside the ad hoc network should be paid more attention, and mobile nodes and infrastructure should not easily trust any node in the network even if it behaves well before because it might have been compromised.

c.) Lack of Centralized Management Facility

Ad hoc networks do not have a centralized piece of management machinery such as a name server, which lead to some vulnerable problems. Now let us discuss this problem in a more detailed manner.

First of all, the absence of centralized management machinery makes the detection of attacks a very difficult problem because it is not easy to monitor the traffic in a highly dynamic and large scale ad hoc network [7]. It is rather common in the ad hoc network that benign failures, such as path breakages, transmission impairments and packet dropping, happen frequently.

Therefore, malicious failures will be more difficult to detect, especially when adversaries change their attack pattern and their attack target in different periods of time. For each of the victims, because it can only observe the failure that occurs in itself, this short-time observation cannot produce a convincing conclusion that the failure is caused by an adversary.

However, we can easily find from a system point of view that the adversary has performed such a large amount of misbehaviors that we can safely conclude that all of the failures caused by this adversary should be malicious failure instead of benign failure, though these failures occur in different nodes at different time. From this example we find that lack of centralized management machinery will cause severe problems when we try to detect the attacks in the ad hoc network.

Second, lack of centralized management machinery will impede the trust management for the nodes in the ad hoc network. In mobile ad hoc network, all the nodes are required to cooperate in the network operation, while no security association (SA2) can be assumed for all

the network nodes. Thus, it is not practical to perform an *a priori* classification, and as a result, the usual practice of establishing a line of defense, which distinguishes nodes as trusted and non trusted, cannot be achieved here in the mobile ad hoc network.

Third, some algorithms in the mobile ad hoc network rely on the cooperative participation of

all nodes and the infrastructure. Because there is no centralized authority, and decision making in mobile ad hoc network is sometimes decentralized, the adversary can make use of this vulnerability and perform some attacks that can break the cooperative algorithm.

In one word, the absence of centralized management machinery will cause vulnerability that can influence several aspects of operations in the mobile ad hoc network.

D.) Restricted Power Supply

As we all know, due to the mobility of nodes in the ad hoc network, it is common that the nodes in the ad hoc network will reply on battery as their power supply method. While nodes in the wired network do not need to consider the power supply problem because they can get electric power supply from the outlets, which generally mean that their power supply should be approximately infinite; the nodes in the mobile ad hoc network need to consider the restricted battery power, which will cause several problems.

The first problem that may be caused by the restricted power supply is denial-of-service attacks [4]. Since the adversary knows that the target node is battery-restricted, either it can continuously send additional packets to the target and ask it routing those additional packets,

or it can induce the target to be trapped in some kind of time-consuming computations. In this way, the battery power of the target node will be exhausted by these meaningless tasks, and thus the target node will be out of service to all the benign service requests since it has run out
of power.
Furthermore, a node in the mobile ad hoc network may behave in a selfish manner when it
finds that there is only limited power supply, and the selfishness can cause some problems when there is a need for this node to cooperate with other nodes to support some functions in the network. Just take the cluster-based intrusion detection technique as an example [8]. In this technique, there is no need that every node in the ad hoc network is the monitoring node all the time; instead, a *cluster* of neighboring MANET nodes can randomly and fairly elect a monitoring node that will observe the abnormal behaviors in the network traffic for the entire cluster. However, an important precondition for the success of this technique is that every node in the cluster is willing to take their responsibility as a monitoring node and serve for all other nodes in a period of time. There may be some nodes that behave selfishly and do not want to cooperate in the monitoring node election process, which will make the election fail if there are too many selfish nodes. Moreover, we should not view all of the selfish nodes as malicious nodes: some nodes may encounter restricted power supply problem and thus behave in a selfish manner, which can be tolerated; however, there can be some other node who intentionally announces that it runs out of battery power and therefore do not want to cooperate with other nodes in some cooperative operation, but actually this node still has enough battery power to support the cooperative operation. In a word, selfish behaviors should not be regarded as malicious behaviors, but we need to know if the selfishness is really caused by the limited battery power, or by the intentional non-cooperation.

E.) Scalability

Finally, we need to address the scalability problem when we discuss the vulnerabilities in the mobile ad hoc network [4]. Unlike the traditional wired network in that its scale is generally predefined when it is designed and will not change much during the use, the scale of the ad hoc network keeps changing all the time: because of the mobility of the nodes in the mobile ad hoc network, you can hardly predict how many nodes there will be in the network in the future. As a result, the protocols and services that are applied to the ad hoc network such as routing protocol and key management service should be compatible to the continuously changing scale of the ad hoc network, which may range from decades of nodes to hundreds of
nodes, or even thousands of nodes. In other words, these protocols and services need to scale
up and down efficiently.

III ATTACKS ON AD HOC NETWORK

There are various types of attacks on ad hoc network which are describing following:
Location Disclosure: Location disclosure is an attack that targets the privacy requirements of an ad hoc network. Through the use of traffic analysis techniques [20], or with simpler probing and monitoring approaches, an attacker is able to discover thelocation of a node, or even the structure of the entire network.

*Black Hole***:** In a black hole attack a malicious node injects false route replies to the route requests it receives, advertising itself as having the shortest path to a destination[26]. These fake replies can be fabricated to divert network traffic through the malicious node for eavesdropping, or simply to attract all traffic to it in order to perform a denial of service attack by dropping the received packets.

Replay: An attacker that performs a replay attack injects into the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions.

*Wormhole***:** The wormhole attack is one of the most powerful presented here since it involves the cooperation between two malicious nodes that participate in the network [53]. One attacker, e.g. node A, captures routing traffic at one point of the network and tunnels them to another point in the network, to node B, for example, that shares a private communication link with A. Node B then selectively injects tunneled traffic back into the network. The connectivity of the nodes that have established routes over the wormhole
link is completely under the control of the two colluding attackers. The solution to the wormhole attack is *packet leashes*.

Blackmail: This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender [58]. An attacker may

fabricate such reporting messages and try to isolate legitimate nodes from the network. The security property of non-repudiation can prove to be useful in such cases since it binds a node to the messages it generated

Denial of Service: Denial of service attacks aim at the complete disruption of the routing function and therefore the entire operation of the ad hoc network [15]. Specific instances of denial of service attacks include the *routing table overflow and* the *sleep deprivation torture.*. In a routing table overflow attack the malicious node floods the network with bogus route creation packets in order to consume the resources of the participating nodes and disrupt the establishment of legitimate routes. The sleep deprivation torture attack aims at the consumption of batteries of a specific node by constantly keeping it engaged in routing decisions.

Routing Table Poisoning: Routing protocols maintain tables that hold information regarding routes of the network. In poisoning attacks the malicious nodes generate and send fabricated signaling traffic, or modify legitimate messages from other nodes, in order to create false entries in the tables of the participating nodes [15]. For example, an attacker can send routing updates that do not correspond to actual changes in the topology of the ad hoc network. Routing table poisoning attacks can result in the selection of non-optimal routes, the creation of routing loops, bottlenecks, and even portioning certain parts of the network.

*Rushing Attack***:** Rushing attack is that results in denial-of-service when used against *all* previous on-demand ad hoc network routing protocols [55]. For example, DSR, AODV, and secure protocols based on them, such as Ariadne, ARAN, and SAODV, are unable to discover routes longer than two hops when subject to this attack. develop *Rushing Attack Prevention (RAP)*, a generic defense against the rushing attack for on-demand protocols that can be applied to any existing on-demand routing protocol to allow that protocol to resist the rushing attack.

Breaking the neighbor relationship: An intelligent filter is placed by an intruder on a communication link between two ISs(Information system) could modify or change information in the routing updates or even intercept traffic belonging to any data session

*Masquerading***:** During the neighbor acquisition process, a outside intruder could masquerade an nonexistent or existing IS by attaching itself to communication link and illegally joining in the routing protocol domain by compromising authentication system. The threat of masquerading is almost the same as that of a compromised IS.

*Passive Listening and traffic analysis***:** The intruder could passively gather exposed routing information. Such a attack cannot effect the operation of routing protocol, but it is a breach of user trust to routing the protocol. Thus, sensitive routing information should be protected. However, the confidentiality of user data is not the responsibility of routing protocol

IV SECURITY SCHMES IMPLEMENTED IN THE MOBILE AD HOC NETWORKS

There are many different schemes which are used to secure
the Mobile ad hoc network. Some of these are discussed below:

A.) Intrusion detection Techniques in Manet

Intrusion detection is not a new concept in the network research. Intrusion Detection System (or IDS) generally
detects unwanted manipulations to systems the proposed
architecture of the intrusion detection system

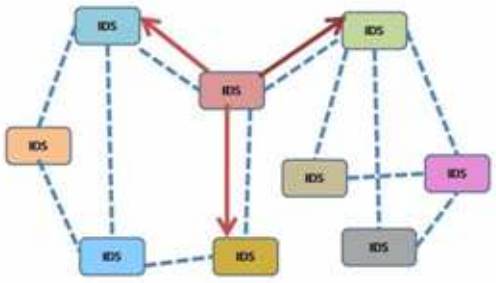

Figure 2

In this architecture, every node in the mobile ad hoc networks participates in the intrusion detection and response activities by detecting signs of intrusion behavior locally and independently, which are performed by the built-in IDS agent. However, the neighboring nodes can share their investigation results with each other and cooperate in a broader range. The cooperation between nodes generally

happens when a certain node detects an anomaly but does not have enough evidence to figure out what kind of intrusion it belongs to. In this Situation, the node that has detected the anomaly requires other nodes in the communication range to perform searches to their security logs in order to track the possible traces of the
intruder. The internal structure of an IDS agent is shown in
following figure

Figure 3

In the conceptual model, there are four main functional
modules:

Local data collection module
This mainly deals with the data gathering issue, in which the real-time audit data may come from various resources.

Local detection engine
Which examines the local data collected by the local data
collection module and inspects if there is any anomaly shown in the data? Because there are always new attack types emerging as the known attacks being recognized by the IDS, the detection engine should not expect to merely perform pattern recognition between known attack behaviours and the anomalies that are likely to be some intrusions: instead of the misuse detection technique that cannot deal with the novel attack types effectively, the detection engine should mainly rely on the statistical anomaly detection techniques, which distinguish anomalies from normal behaviours based on the deviation between the current observation data and the normal profiles of the system.

Cooperative detection engine
Which works with other IDS agents when there are some
needs to find more evidences for some suspicious anomalies detected in some certain nodes? When there is a need to initiate such cooperated detection process, the participants will propagate the intrusion detection state information of themselves to all of their neighbouring nodes, and all of the participants can calculate the new intrusion detection state of them based on all such information they have got from their neighbours by some selected algorithms such as a distributed consensus algorithm with weight. Since we can make such a reasonable assumption that majority of the nodes in the ad hoc network should be benign, we can trust the conclusion drawn by any of the participants that the network is under attack.

Intrusion response module
This deals with the response to the intrusion when it has been confirmed. The response can be reinitializing the communication channel such as reassigning the key, or reorganizing the network and removing all the compromised nodes. The response to the intrusion behaviour varies with the different kinds of intrusion

B.) Cluster-based intrusion Detection technique for Ad hoc networks.

We have discussed cooperative intrusion detection architecture for the ad hoc networks in the previous part,
which was first presented by Zhang et al. However, all of the nodes in this framework are supposed to participate in the cooperative intrusion detection activities when there is such a necessity, which cause huge power consumption for all the participating nodes. Due to the limited power supply in the ad hoc network, this framework may cause some nodes behave in a selfish way and not cooperative with other nodes so as to save their battery power, which will actually violate the original intention of this cooperative intrusion detection architecture. To solve this problem a cluster-based intrusion detection technique is used in this technique A MANET can be organized into a number of clusters in such a way that every node is a member of at least one cluster, and there will be only one node per cluster that will take care of the monitoring issue in a certain period of time, which is generally called **clusterhead**. A cluster is a group of nodes that reside within the same radio range with each other, which means that when a

node is selected as the clusterhead, all of the other nodes in this cluster should be within 1-hop vicinity.
It is necessary to ensure the fairness and efficiency of the
cluster selection process. Here fairness contains two levels of meanings: the probability of every node in the cluster to be selected as the clusterhead should be equal, and each node should act as the cluster node for the same amount of time. Efficiency of the process means that there should be some methods that can select a node from the cluster periodically with high efficiency. The finite state machine of the cluster formation protocol is shown in Figure

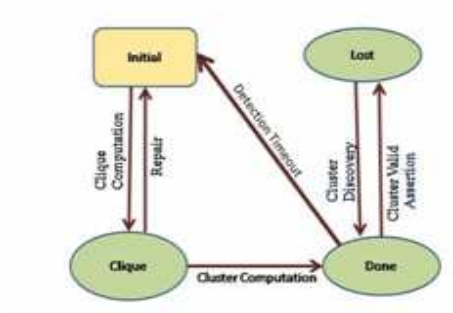

Figure 4

Basically there are four states in the cluster formation protocol: initial, clique, done and lost. All the nodes in the network will be in the initial state at first, which means that they will monitor their own traffic and detect intrusion behaviors independently. There are two steps that we need to finish before we get the cluster head of the network: clique computation and cluster head computation. A clique is defined as a group of nodes where every pair of members can communicate via a direct wireless link. The definition of clique is a little more restricted than that of cluster. Once the protocol is finished, every node is aware of its fellow clique members. Then a node will be randomly selected from the clique to act as the cluster head. There are two other protocols that assist the cluster doing some validation and recovery issues, which are respectively called Cluster Valid Assertion Protocol and Cluster Recovery Protocol. The cluster valid assertion protocol has generally been used in the following two situations:
.
1. The node in the cluster will periodically use the Cluster
Valid Assertion Protocol to check if the connection between the cluster head and itself is maintained or not. If not, this node will check to see if it belongs to another cluster, and if it also get negative answer, then the node will enter the LOST state and initiate a routing recovery request.

2. Furthermore, there need to be a mandatory re-election
timeout for the clusterhead to keep the fairness and security of the whole cluster. If the timeout expires, all the nodes switch from DONE state to INITIAL state and begin a new round of clusterhead election.
The Cluster Recovery Protocol is mainly used in the case that a citizen loses its connection with previous clusterhead or a clusterhead loses all its citizens, when it enters LOST state and initiates Cluster Recovery Protocol to re-discover a new clusterhead.

C.) Misbehaviour detection Through cross-layer analysis

Some *smart* attackers may simultaneously exploit several vulnerabilities at multiple layers but keep the attack to each of the vulnerabilities stay below the detection threshold so as to escape from capture by the single-layer misbehavior detector. This type of cross-layer attack will be far more threatening than the single-layer attack in that it can be easily skipped by the single-layer misbehaviour detector. Nevertheless, this attack scenario can be detected by a crosslayer misbehaviour detector, in which the inputs from all layers of the network stack are combined and analyzed by the cross-layer detector in a comprehensive way. First of all it will be an important problem that how to make the cross-layer detection more efficient, or in other words, how to cooperate between single-layer detectors to make them work well. Because different single-layer detectors deal with different types of attacks, there can be some different viewpoints to the same attack scenario when it is observed in different layers. Therefore it is necessary to figure out the possible solution if there are different detection results generated by different layers. Second, we need to find out how much the system resource and network overhead will be increased due to the use of cross-layer detector compared with the original single layer detector. Due to the limited battery power of the nodes in the ad hoc networks, the system and network overhead brought by the cross-layer detection should be taken into account and compared with the performance gain caused by the use of cross-layer detection method.

V CONCLUSION

The research on MANET security is still in its early stage. The existing proposals are typically attack-oriented in that they first identify several security threats and then enhance the existing protocol or propose a new protocol to thwart such threats. Because the solutions are designed explicitly with certain attack models in mind, they work well in the presence of designated attacks but may collapse under unanticipated attacks. Therefore, a more ambitious goal for ad hoc network security is to develop a multi-fence security solution. protection etc. The Security research area is still open as many of the provided solutions are designed keeping a limited size scenario and limited kind of attacks and vulnerabilities.

VI REFERENCES

[1] Marco Conti, Body, Personal and Local Ad Hoc Wireless Networks, in Book *The Handbook of Ad Hoc Wireless Networks (Chapter 1)*, CRC Press LLC, 2003.

[2] M. Weiser, The Computer for the Twenty-First Century, *Scientific American*, September 1991.

[3] M.S. Corson, J.P. Maker, and J.H. Cernicione, Internet-based Mobile Ad Hoc Networking, *IEEE Internet Computing*, pages 63–70, July-August 1999.

[4] Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book *The Handbook of Ad Hoc Wireless Networks (Chapter 30)*, CRC Press LLC, 2003.

[5] Lidong Zhou and Zygmunt J. Hass, Securing Ad Hoc Networks, *IEEE Networks Special Issue on Network Security*, November/December 1999.

[6] Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book *Ad Hoc Networks Technologies and Protocols (Chapter 9)*, Springer, 2005.

[7] Panagiotis Papadimitraos and Zygmunt J. Hass, Securing Mobile Ad Hoc Networks, in Book *The Handbook of Ad Hoc Wireless Networks (Chapter 31)*, CRC Press LLC, 2003.

[8] Yi-an Huang and Wenke Lee, A Cooperative Intrusion Detection System for Ad Hoc Networks, in *Proceedings of the 1st ACM Workshop on Security of Ad hoc and Sensor Networks*, Fairfax, Virginia, 2003, pp. 135 – 147.

[9] Data Integrity, from *Wikipedia, the free encyclopedia*, http://en.wikipedia.org/wiki/Data_integrity.

[10] P. Papadimitratos and Z. J. Hass, Secure Routing for Mobile Ad Hoc Networks, in Proceedings of *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS)*, San Antonio, TX, January 2002.

[11] Y. Hu, A. Perrig and D. Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks, in *Proceedings of ACM MOBICOM'02*, 2002.

[12] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, A Secure Routing Protocol for Ad Hoc Networks, in *Proceedings of ICNP'02*, 2002.

[13] Y. Hu, D. Johnson, and A. Perrig, SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks, *Ad Hoc Networks*, 1 (1): 175–192, July 2003.

[14] Y. Hu, A. Perrig and D. Johnson, Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks, in *Proceedings of IEEE INFOCOM'03*, 2003.