International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 02 (MAR-APR, 2016)

Survey of APT and other Attacks with Reliable Security Schemes in MANET

Batika Rai
M Tech. Pursuing of Dept. of CSE
RITS, Bhopal
rai.batika@gmail.com

Prof. Anurag Jain
Dept. of CSE
RITS, Bhopal
Anurag.akjain@gmail.com

***Abstract*— The Mobile Ad hoc Network (MANET) is forming the temporary network without any supervision of any administration. The attacker can easily corrupt the information of this dynamic network because of absence of supervision system. The routing is a problem in a decentralize environment where the topology fluctuate the node easily moves in an environment. In MANET, all networking functions such as routing and packet forwarding, are performed by nodes themselves like a self-organizing manner. For these reasons, securing a mobile ad hoc network is very difficult. The Advanced Persistent Thread (APT) detects the malware misbehavior in network like virus, Trojan and worms. The term "Advanced Persistent Threat" is used for a variety of cyber threats. This specific characteristic of MANET has provided it susceptible to security attacks which results in degradation in the performance characteristics as well as raises a serious problem about the reliability of such networks. In MANET, uncooperative node is malicious node that functions as a malware and infected the network performance. The nodes that are faulty and therefore cannot follow a protocol, or are intentionally malicious and try to attack the system. The Intrusion Detection System (IDS) can secure network from APT but difficult to design it. In this paper, we will address the different types of attacks and their security schemes. There is no work is done to protect MANET from unauthorized access through APT. These attacks can degrade the network performance and also the security schemes that are protecting the network from attacks.**

***Keywords*- MANET, AODV, Malicious node, routing, security**

I. INTRODUCTION

Mobile ad hoc networks (MANETs) are maintain the temporary connection between the mobile stations or hosts having the capability of routing can established connection without any fixed infrastructure. APT are among the most serious information security threats that organizations face today. Goal of an APT is to steal intellectual property (IP) from the targeted organization, to gain access to customer data, or to access strategic business information that could be used for financial gain, blackmail, and embarrassment, data poisoning, illegal insider trading or disrupting an organization's business. Viruses, worms, Trojans, and bots are all part of a class of software called malware. Malware or malicious code (malcode) is short for malicious software. It is code or software that is specifically designed to damage, disrupt, steal, or in general inflict some other "bad" or illegitimate action on data, hosts, or networks. The dynamic topology of MANET allows nodes to join and leave the network at any point of time. The network is decentralized, where network organization and message delivery must be executed by the nodes themselves. There are many efforts have done to surviving MANETs and keep them to provide services even in the presence of intrusion and attacks [2]. Figure 1 represents communication between the nodes in MANET environment.

Fig. 1 Mobile Ad hoc Network

The nature of ubiquitous devices makes wireless networks the easiest solution for their interconnection and, as a consequence, the wireless arena has been experiencing exponential growth in the past decade. Mobile users can use their cellular phone to check e-mail, browse internet; travelers with portable computers can surf the internet from airports, railway stations, Starbucks and other public locations [1] has many characteristic which make it suitable for some important applications and it can provide services well in such cases. Mobile ad hoc network have become an important part of our life due to its vital services which provided to the population and society. It used at home, work, emergency situation, and natural disaster. On the other hand, the threats of MANET have flourished too. Not only are mobile devices get getting smaller, cheaper, more convenient, and more powerful, they also run more applications and network services, commonly fueling the explosive growth of mobile computing equipment market. The exploding number of Internet and laptop users driving this growth further enhanced. Projections show that in the recent years the number of mobile connections and the number of shipments of mobile and Internet terminals will grow yet by another 95% in recent time. With this trend, we can expect the total number of mobile Internet users soon to exceed that of the fixed-line Internet users. Advanced Persistent Threat (APT) [3, 4] is a term referring to targeted attacks on enterprises and other organizations. These attacks use commercially available and custom-made advanced malware to steal information or perpetrate

fraud. Legacy perimeter and endpoint security controls, such as firewalls, AV gateways and AV desktop clients, are unable to stop advanced threats. Advanced malware uses a myriad of attack tactics to execute an APT. Spear phishing is typically used to lure targeted users to infected web sites or social engineer them to download infected documents. The security mechanism for MANET, on one hand, must require low computation complexity and a small number of appended messages to save limited resources. On the other hand, it should also be competitive and effective in preventing misbehaviors through virus, worms and malware or identifying misbehaving nodes from normal ones. Cyber-attacks against companies and governments are seeing an increase in complexity and persistence. These more complex attacks are aimed at penetrating corporate and government networks to obtain classified information. The difference with cyber attacks from a couple of years ago is that attackers take more time and effort to remain undetected.

Attacks on MANET are classified as Active and Passive attacks [5], passive attacks are not dangerous if the delivering data is important than its security, because it does not affects the normal operation of MANET, while active attacks affecting the normal operation of MANET In several ways. This survey focusing on initiatives which make MANET survives against active attacks.

II. Requirements against APT

The APT is the multiple kind of misbehavior happening in dynamic network. The network security is necessary to protect confidential data from unauthorized users i.e. possible by APT in network. The requirements against of APT [6] are as follows:-

A. Protect Application Clients and Browsers Against Exploitation and Tampering

Browsers and Application clients on managed and unmanaged devices must be protected against advanced malware. Attempts to exploit browser, client and operating system services and gain access to enterprise resources should be detected, prevented and reported to IT security.

B. Protect the Browser against Reconnaissance and Social Engineering

Many organizations leverage browser-based access to corporate applications, which are susceptible to Man-in-the-Browser attacks such as session logging and malicious web page injection. Session logging captures login credentials and provides broad access to sensitive corporate data and applications. And, it can also capture raw data accessed by end users. Web injection is used to social engineer employees into surrendering credentials and other confidential information. End users should be protected against these attack vectors to secure access to sensitive data.

C. Stop "Back Doors" and Data Leaks

Remote Access Trojans (RATs) provide cybercriminals with unlimited access to infected endpoints. Using the victim's access privileges, they can leverage an active strongly authenticated session, wherever the endpoint is located, to steal sensitive business and personal data including intellectual property and personally identifiable information (PII). Security tools must detect the presence of malicious RATs and stop the execution of remote access sessions into the endpoint.

D. Block Malware Infection, Remove Existing Malware

Controls should be implemented to prevent malware from infecting managed and unmanaged devices that access the enterprise. If infected, automated removal of existing malware from end-users machines will streamline support efforts. Special focus should be given to resource consumption and management overhead when balancing strength of the protection and risk reduction with end user and IT security impact.

E. Enterprise Controlled Deployment and Management

Protection against advanced malware used in APT attacks must cover the vast majority of managed and unmanaged device platforms, including PCs, Macs and Mobile (iOS and Android devices). For unmanaged devices, an on demand deployment option must be readily available to end users to instantly secure ad-hoc and personal devices that need to access corporate data. Organizations must have the ability to mandate that all access be performed from secured endpoint (i.e. ensure that an endpoint security control in installed and functioning).

III. Malware attack and Types

The word "malware" is short for "malicious software." Many people use the word "virus" to indicate any type of harmful software, but a virus is actually just a specific type of malware [7]. There are many different classes of malware that have varying ways of infecting systems and propagating themselves. Malware can infect systems by being bundled with other programs or attached as macros to files. Others are installed by exploiting a known vulnerability in an operating system (OS), network device, or other software, such as a hole in a browser that only requires users to visit a website to infect their computers. The vast majority, however, are installed by some action from a user, such as clicking an e-mail attachment or downloading a file from the Internet. Some of the more commonly known types of malware are viruses, worms, Trojans, bots, back doors, spyware, and adware. Damage from malware varies from causing minor irritation (such as browser popup ads), to stealing confidential information or money, destroying data, and compromising and/or entirely disabling systems and networks. Malware cannot damage the physical hardware of systems and network equipment, but it can damage the data and software residing on the equipment. Malware

should also not be confused with defective software, which is intended for legitimate purposes but has errors or bugs. The word "malware" encompasses all harmful software, including all the ones listed below.

A. Classes of Malicious Software

Two of the most common types of malware are viruses and worms. These types of programs are able to self-replicate and can spread copies of themselves, which might even be modified copies. To be classified as a virus or worm, malware must have the ability to propagate. The difference is that a worm operates more or less independently of other files, whereas a virus depends on a host program to spread itself. These and other classes of malicious software are described below.

*1) Viruses:-*A computer virus is a type of malware that propagates by inserting a copy of itself into and becoming part of another program. It spreads from one computer to another, leaving infections as it travels. Viruses can range in severity from causing mildly annoying effects to damaging data or software and causing denial-of-service (DoS) conditions. Almost all viruses are attached to an executable file, which means the virus may exist on a system but will not be active or able to spread until a user runs or opens the malicious host file or program. When the host code is executed, the viral code is executed as well. Normally, the host program keeps functioning after it is infected by the virus. However, some viruses overwrite other programs with copies of themselves, which destroys the host program altogether. Viruses spread when the software or document they are attached to is transferred from one computer to another using the network, a disk, file sharing, or infected e-mail attachments.

2) *Worms:-*Computer worms are similar to viruses in that they replicate functional copies of themselves and can cause the same type of damage. In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate. To spread, worms either exploit vulnerability on the target system or use some kind of social engineering to trick users into executing them. A worm enters a computer through vulnerability in the system and takes advantage of file-transport or information-transport features on the system, allowing it to travel unaided. Some well known examples of worms are the famous "Iloveyou" and "conficker" worms.

3) Trojans:- A Trojan is another type of malware named after the wooden horse the Greeks used to infiltrate Troy. It is a harmful piece of software that looks legitimate. Users are typically tricked into loading and executing it on their systems. After it is activated, it can achieve any number of attacks on the host, from irritating the user (popping up windows or changing desktops) to damaging the host (deleting files, stealing data, or activating and spreading other malware, such as viruses). Trojans are also known to create back doors to give malicious users access to the system. Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate. Trojans must spread through user interaction such as opening an e-mail attachment or downloading and running a file from the Internet.

4) Bots:- "Bot" is derived from the word "robot" and is an automated process that interacts with other network services. Bots often automate tasks and provide information or services that would otherwise be conducted by a human being. A typical use of bots is to gather information (such as web crawlers), or interact automatically with instant messaging (IM), Internet Relay Chat (IRC), or other web interfaces. They may also be used to interact dynamically with websites. Bots can be used for either good or malicious intent. A malicious bot is self-propagating malware designed to infect a host and connect back to a central server or servers that act as a command and control (C&C) center for an entire network of compromised devices, or "botnet." With a botnet, attackers can launch broad-based, "remote-control," flood-type attacks against their target(s). In addition to the worm-like ability to self-propagate, bots can include the ability to log keystrokes, gather passwords, capture and analyze packets, gather financial information, launch DoS attacks, relay spam, and open back doors on the infected host. Bots have all the advantages of worms, but are generally much more versatile in their infection vector, and are often modified within hours of publication of a new exploit. They have been known to exploit back doors opened by worms and viruses, which allows them to access networks that have good perimeter control. Bots rarely announce their presence with high scan rates, which damage network infrastructure; instead they infect networks in a way that escapes immediate notice.

B. Best Practices for Combating Viruses, Worms, Trojans, and Bots

The first steps to protecting your computer are to ensure that your OS is up to date. This means regularly applying the most recent patches and fixes recommended by the OS vendor. Secondly, you should have antivirus software installed on your system and download updates frequently to ensure that your software has the latest fixes for new viruses, worms, Trojans, and bots. Additionally, you want to make sure that your antivirus program can scan e-mail and files as they are downloaded from the Internet. This will help prevent malicious programs from reaching your computer. You may also want to consider installing a firewall.

C. Additional Definitions and References

1) Exploit:- An exploit is a piece of software, a command, or a methodology that attacks particular security vulnerability. Exploits are not always malicious in intent—they are

sometimes used only as a way of demonstrating that vulnerability exists. However, they are a common component of malware.

2) *Back Door*:- A back door is an undocumented way of accessing a system, bypassing the normal authentication mechanisms. Some back doors are placed in the software by the original programmer and others are placed on systems through a system compromise, such as a virus or worm. Usually, attackers use back doors for easier and continued access to a system after it has been compromised.

IV. Routing in MANET

Routing is essential service for end-to-end communication in MANET, attacks on routing protocol disrupt the reliability and performance of MANET. It can be divided into two categories, first is routing disruption attack which the attacker trying to change the course of packets. Second resource consumption attack, the attacker inserts packet into the network to consume resources [2]. According to how the information is acquired, the routing protocols can be classified into proactive, reactive and hybrid routing [8, 9].

A. Proactive (table-driven) Routing Protocol

The proactive routing is also known as table-driven routing protocol. In this routing protocol, mobile nodes periodically broadcast their routing information to the neighbor's nodes. Each node needs to maintain their routing table of not only adjacent nodes and reachable nodes but also the number of hops. Therefore, the disadvantage is the rise of overhead due to increase in network size, a significant big communication overhead within a larger network topology. However, the major advantage is of knowing the network status immediately if any malicious attacker joins. The most familiar types of the proactive routing protocol are: - Destination sequenced distance vector (DSDV) routing protocol and Optimized link state routing (OLSR) protocol.

B. Reactive (on-demand) Routing Protocol

The reactive routing protocol is equipped with another appellation named on-demand routing protocol. In compare to the proactive routing, the reactive routing is simply starts when nodes desire to transmit data packets. The major advantage is the reduction of the wasted bandwidth induced from the cyclically broadcast. The disadvantage of reactive routing protocol method is loss of some packet. Here we briefly describe two prevalent on-demand routing protocols which are: - Ad hoc on-demand distance vector (AODV) and Dynamic source routing (DSR) protocol.

C. Hybrid Routing Protocol

The hybrid routing protocol as the name suggests have the combine advantages of proactive routing and reactive routing to overcome the defects generated from both the protocol when used separately. Design of hybrid routing protocols are mostly as hierarchical or layered network framework. In this system initially, proactive routing is employed to collect unfamiliar routing information, and then at later stage reactive routing is used to maintain the routing information when network topology changes. The familiar hybrid routing protocols are: - Zone routing protocol (ZRP) and Temporally-ordered routing algorithm (TORA).

V. Types of Attacks in NAMET

The action of an a attacker includes injecting packets to invalid destinations into the network, deleting packets, modifying the contents of packets, The attacks and their behavior are mentioned in [2, 5, 10].

Flooding Attack: This type of attack intends to consumption node resources significantly such as bandwidth and battery power, or disrupting the normal routing operation. Flooding attack can happened when a malicious node send a large number of Route-Request (RREQ) packets in a very short time to a none existent node and there will not be Route-Replay (RREP), so the (RREQs) will flood network. As a result the throughput decreasing significantly; or flooding the destination node with a large number of unnecessary packets, it cannot receive all packets therefore all packets will discard.

Wormhole Attack: This type of attack occur when an attacker tunnel the routing control message to another location using a high speed communication link to prevent the completion of routing discovery process. This attack is one of the most sever attacks encounter mobile ad hoc network, it can overcome the authenticity and confidentiality communication, this shows the seriousness of this attack.

Rushing Attack: Rushing attack is a special type of wormhole attack occurred if a fast channel dedicated between two wormhole nodes, it intend to attack on-demand routing protocols that use duplicate suppression at each node used by many wireless routing protocols. In rushing attack, the adversary node floods the RREQ packet faster than other nodes which make legitimate nodes receive the same packets twice it assume these legitimate RREQs are duplicate packets and it is simply discard. Source node considers that adversary node as normal intermediate node, therefore source node could not find the route path that do not including adversary node. The most dangerous attacks against MANET routing protocols which results in Denial of service is rushing attack, because the shared high speed transmission path between two end wormhole nodes which called rushing attack prevent current secure routing protocols from discovering route more than two hops. The other thing makes rushing attack dangerous that it can perform also by week attackers.

Black Hole Attack: In this attack, the malicious node pretend that it is a legitimate node and it has a valid route to the destination node, therefore the source node will select it,

although it does not has a valid route. Black hole attack intends to damage or prevent some of forwarded packets while leaving some packets undamaged.

Byzantine Attack: A malicious intermediate nodes works alone or colluding to perform routing problems such as selecting a non-optimal path to forwarding packets or creating routing loops for packets or dropping a selected packets which results in significantly of throughput degradation or routing disruption.

VI. SECURITY AGAINST ATTACKS

For the MANET security, the following attributes: availability, confidentiality, integrity, authentication, and non-repudiation need to be considered [11].

Availability: Availability is ensures the survivability of network services despite denial-of-service attacks. An attack can be launched at any layer of an ad hoc network. An adversary could employ jamming to interfere with communication on the physical and media access control layers; disrupt the routing protocol and disconnect the network on the network layer; bring down high-level services on the higher layer. One useful measure is the key management service not only for ad hoc network, but also for traditional network.

Confidentiality: Confidentiality is ensures that certain information is never disclosed to unauthorized entities. Such information includes network transmission of sensitive information and routing information. Due to the inherent characteristic of ad hoc networks, each node acts as a router, and sensitive information needs multi-hop paths through network to other nodes, thereby enlarging the possibility of leaking routing information.

Integrity: Integrity requires that messages should not be altered or corrupted during transmission. A message could be altered by a benign or malicious attack on the network.

Authentication: Authentication means that the participants somehow prove that their identities are what they claim them to be. Authentication can be done by something users know, embody or possess. For instance, something known can be a password, something embodied can be a fingerprint, and something possessed can be a smart card.

Non-repudiation: Non-repudiation guarantees that the origin of a message cannot deny having sent the message and the receiver cannot deny the reception. Non-repudiation is useful for detection and isolation of compromised nodes. For instance, when node A receives an erroneous message from node B, non-repudiation allows A to accuse B using this message and to convince other nodes that B is compromised. Non-repudiation as a property or requirement is not achievable overall (at least extremely difficult to achieve). The security community often demands a weaker condition in order to meet the reality. Based on the above-mentioned requirements, several traditional security mechanisms still play important roles in achieving above attributes. Changes need to be added to these mechanisms. We will discuss the details in the rest of the paper.

Encryption: Encryption can be used to hide the information during transmission or to store information more safely. It is assumed to change the information in such a way that only authorized users can interpret it. Therefore, encryption is used to gain confidentiality. Protocols Encryption alone does not accomplish security. It works as a part of the security protocol used in a network. The protocol defines the steps how, for example, the parties authenticate each other, and what infrastructure is needed for the authentication. Protocols involve key management, and they may often require the use of certificates.

User authentication and access control methods: The access control rights can be kept with the subjects (e.g. the users) or the objects (e.g. the resources). Both methods may take advantage of certificates. Certificates may be used to identify an entity associated with a cryptographic key or to specify the access rights to be given to the holder of a cryptographic key.

Physical security and firewalls: A firewall is a security system that protects the boundary of an internal network. Basically, all the traffic leaving and entering the internal network is routed through one node, and the security controls are constructed to this point. The firewall may control access to the services of the internal network, hide the internal network (topology, addresses, and traffic) from the outside world, check for viruses in incoming files, and add cryptographic protection to data leaving the network.

VII. .PREVIOUS SOLUTIONS AGAINST ATTACK

In this section the previous work done in field of APT and security in MANET is mention but the no research is done in field of MANET to secure with APT. In this part we mention the previous work separately. In this paper [12], the model and algorithm for detecting the latest APT attacks were proposed. Separate the patterns normally used by the organization member and abnormal patterns to narrow the detection range sufficiently. For that, all outbound traffic types within a specific period must be investigated, and acceptance of the investigated traffic should be manually judged within the organization. The proposed model and algorithm were tested in a small office environment and verified to be somewhat effective. This paper [13] was focused on the impact of traditional Information and Communications Technologies (ICT) mal ware on Supervisory Control and Data Acquisition (SCADA) systems. Additionally, it presents examples of computer malware designed to attack a typical SCADA system, and discusses their potential damaging effects. Malware poses a serious threat to SCADA systems and the industrial facilities they control. Since it is dangerous to infect a real SCADA system with malware, the most appropriate strategy

for analyzing the effects of malware is to use a simulation framework that can mimic its behavior. In [14] the authors have introduced the route confirmation request (CREQ) and route confirmation reply (CREP) to avoid the black hole attack. In this approach, the intermediate node not only sends RREPs to the source node but also sends CREQs to its next-hop node toward the destination node. After receiving a CREQ, the next-hop node looks up its cache for a route to the destination. If it has the route, it sends the CREP to the source node. Upon receiving the CREP, the source node can confirm the validity of the path by comparing the path in RREP and the one in CREP. If both are matched, the source node judges that the route is correct. One drawback of this approach is that it cannot avoid the black hole attack in which two consecutive nodes work in collusion, that is, when the next-hop node is a colluding attacker sending CREPs that support the incorrect path. In [15] Authors Ming-Yang Su et.al discussed a mechanism known as ABM (Anti-Black hole Mechanism), which is mainly used to estimate the suspicious value of a node according to the amount of abnormal difference between RREQs and RREPs transmitted from the node. When a suspicious value exceeds the limit, the nearby IDS broadcasted a block message with id of IDS, the identified black hole node and the time of identification will place the malicious nodes on their blacklists to isolate the malicious node in the network cooperatively. The advantage of this method is that it can be able to detect cooperative black hole nodes in the MANETs. The main drawback of this technique is that mobile nodes have to maintain an extra database for training data and its updating, in addition to the maintenance of their routing table. In [16] this scheme trust based communication in MANET using AOMDV-IDS against the black hole attack. AOMDV-IDS perform real time detection of attacks using AOMDV routing protocol. In AOMDV, RREQ transmission from the source to the target establishes multiple reverse paths both at intermediary nodes in addition to the destination. Multiple RREPs navigates this reverse route back to from multiple onward routes to the target at the source and intermediary nodes. Multiple routes revealed are loop-free and disjoint. AOMDV depends on the routing information previously available in the AODV protocol, thus preventing the overhead acquired in determining multiple paths. In [17] Message Security Using Trust-Based Multipath Routing (TMR) provides a method of message security using trust-based multipath routing. In this approach, less trusted nodes are given lesser number of self-encrypted parts of a message, thereby making it difficult for malicious nodes to gain access to the minimum information required to break through the encryption strategy. Using trust levels, it makes multipath routing flexible enough to be usable in networks with vital nodes and absence of necessary redundancy. In addition, using trust levels, it avoids the non-trusted nodes in the routes that may use brute force attacks and may decrypt messages if enough parts of the message are available to them. This technique uses a variation of the trust models used in [18] and [19]. A node is assigned a discrete trust level in the range of -l to 4. A trust level -l of 4 defines a complete trust and a trust level of – 1 defines a complete distrust. These trust levels also define the maximum number of packets which can be routed through those nodes. The trust level assigned to a node is a combination of direct interaction with its neighbors and the recommendations from its peers. A node assigns a direct trust level to its neighbors on the basis of acknowledgements received. In [19] Security Enhancement through Multipath Transmission (DMR) provides a way to further secure the data transmitted along routes of a wireless ad hoc network after a potentially secure connection has been established between two nodes. In this method, the encryption/decryption key used is the message itself. The approach requires that the message is split into parts (sub messages) and that the encrypted sub messages be transmitted along different paths (routes) which are reception disjoint. The method partitions a 4n-bit message into two four n-bit parts called *a, b, c, d*. Up to three redundant bits can be added in order to make the number of bits a multiple of four. Four encrypted n-bit parts, labeled *a', b', c', d'* are generated using the equations referred in [19]. Watchdog and path rater approach is proposed [20] to detect and isolate the misbehaving nodes. In this approach, a node forwarding a packet checks if the next hop also forwards it. If not, a failure count is incremented and the upstream node is rated to be malicious if the count exceeds a certain threshold. The path rater module then utilizes this knowledge to avoid it in path selection. It improves the throughput of the network in the presence of malicious nodes. However, it has the demerit of not penalizing the malicious nodes. In [21] have suggests that despite the fact that networks only function properly if the participating nodes cooperate in routing and forwarding. However, it may be advantageous for individual nodes not to cooperate. They propose a protocol, called CONFIDANT, which aims at detecting and isolating misbehaving nodes, thus making misbehavior unattractive. Here misbehaving nodes are excluded from forwarding routes. It includes a trust manager to evaluate the level of trust of alert reports. But it is not clear how fast the trust level can be adjusted for compromised node especially if it has a high trust level initially [22]. In [23] had proposed a new Intrusion Detection System (IDS) based on Mobile Agents. The approach uses a set of Mobile Agent (MA) that can move from one node to another node within a network. This as a whole reduces network bandwidth consumption by moving the computation for data analysis to the location of the intrusion. Besides, it has been established that the proposed method also decreases the computation overhead in each node in the network. In [24] had proposed a scheme which not only confirms the security of data but also guarantees the uninterrupted operation of agent by utilizing a dummy agent and composite acknowledgement technique. Their simulation

also shows that no agent blocked for any number of faulty nodes. Some draw back shows the increase in delay, they have not considered the security of monitoring agent, the processing time needed is also higher. They surveyed three approaches for the problem of mobile agent protection. The three approaches are chosen because each approach is very uniquely implemented and has strengths that other approaches do not have; they choose Partial result authentication code approach because it can protect results from mobile agents. Computing with encrypted functions approaches is chosen because it tries to scramble code and data together. An obfuscated code approach is chosen because it scrambles an agent's code in such a way that no one is able to gain a complete understanding of its function.

VIII. Expected Outcome

It has been observed that although active research is being carried out in this area, the proposed solutions are not complete in terms of effective and efficient routing security. There are limitations on all solutions. They may be of high computational or communication overhead In future we try to proposed Intrusion Detection System (IDS) can collect and analyze audit data for the entire network. So according to that above definition we conclude MANET is distributed nature and can't trust to any of the mobile devices because we cannot manage the every time of topology changes on the network. This is very big challenge. So that particular point we create the trust based routing against the malicious attack in MANET. Destructive malware can utilize popular communication tools to spread, including worms sent through email and instant messages, Trojan horses dropped from web sites, and virus-infected files downloaded from peer-to-peer connections. Malware will also seek to exploit existing vulnerabilities on systems making their entry quiet and easy. The proposed security scheme in future is based on the APT because of the protect network from virus, worms and Trojan horse. The all three attacks have different functioning and IDS against APT is providing security to stop their malicious activities.

IX. Conclusion

In Decentralized dynamic network called MANET, providing security is a critical issue. The primary limitation of the MANETs is the limited resource capability like bandwidth, power back up and computational capacity. In this survey we highlights the some malicious Malware includes viruses, worms, Trojan horses, Bot, Backdoor and other malicious programs in to infected the nodes performance in dynamic network and the attacks in MANET. The majority of active malware threats are usually rootkits, worms or Trojans rather than actual viruses. Absence of infrastructure, changing topology makes the security of MANETs particularly difficult. Also no centralized authority is present to monitor the networking operations of these attacks, the passive attacks do not disrupt the operation of a protocol, but is only information seeking in nature whereas active attacks disrupt the normal operation of the MANET as a whole by targeting specific node(s). In this survey, we reviewed the types of malware like virus worms Trojan horse and bots malicious functioning and current state of the routing attacks and countermeasures MANETs. The APT has a capability to block the performances and IDS against provides the secure communication through mobile nodes in MANET

References

[1] Macro Conti, Silvia Giordano and Ivan Stojmenovi "Mobile Ad Hoc Networks", Stefano Basagni, IEEE press, A john Wily & Sons, INC. publication, 2003

[2] A.K. Rai, R. R. Tewari and S. K. Upadhyay, "Different Types of Attacks on Integrated MANET-Internet Communication," International Journal of Computer Science and Security, Vol. 4, No. 3, 2010, pp. 265-274.

[3] GOVCERT.NL, "Cyber security beheld Nederland," GOVCERT.nl, Den Haag, 2012.

[4] V. Igure and R. Williams, "Taxonomies of Attacks and Vulnerabilities in Computer Systems," IEEE Communications Surveys & Tutorials, vol. 10, no. 1, pp. 6-19, 2008

[5] [3] B. Wu, J. M. Chen, J. Wu and M. Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks," Wireless/Mobile Network Security, Springer, Berlin, 2007, pp. 103-135.

[6] http://www.trusteer.com/glossary/advanced-persistent-threat-apt

[7] ww.cisco.com/web/about/security/intelligence/virus-worm-diffs.html

[8] [7]Sunil Taneja and Ashwani Kush "A Survey of Routing Protocols in Mobile Ad Hoc Networks", International Journal of Innovation, Management and Technology, Vol. 1, No. 3, pp. 279-285, August 2010.

[9] Ipsita Panda "A Survey on Routing Protocols of MANETs by Using QoS Metrics" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, pp. 121-129, 2012

[10] Noman Mohammed, Hadi Otrok, Lingyu Wang, Mourad Debbabi and Prabir Bhattacharya "Mechanism Design- Based Secure Leader Election Model for Intrusion Detection in MANET", IEEE Transactions on Dependable and Secure Computing, vol. 99, no. 1, 2008.

[11] W. Stallings, "Cryptography and Network Security", Principles and Practices, 3rd edition, Prentice Hall, 2003.

[12] Jisang Kim1, Taejin Lee, Hyung-guen Kim, Haeryong Park, " Detection of Advanced Persistent Threat by Analyzing the Big Data Log", Advanced Science and Technology Letters Vol.29, pp.30-36 , SecTech 2013.

[13] Igor Nai Fovinoa, Andrea Carcanoa, Marcelo Maseraa, Alberto Trombettab "An Experimental Investigation of Malware Attacks on SCADA Systems" International Journal of Critical Infrastructure Protection 2, (Elsevier), pp. 139-145, 2009.

[14] Seungjoon Lee, Bohyung Han, Minho Shin; "Robust Routing in Wireless Ad Hoc Networks" 2002, international Conference.

[15] Ming-Yang Su; Kun-Lin Chiang; Wei-Cheng Liao, "Mitigation of Black-Hole Nodes in Mobile Ad Hoc Networks," Parallel and Distributed Processing with Applications (ISPA), 2010 International Symposium on, vol., no., pp.162-167, 6-9 Sept. 2010.

[16] Akanksha Jain, "Trust Based Routing Mechanism against Black Hole Attack using AOMODV-IDS System In MANET Format" IJETAE, Vol. 2, April 2012.

[17] P. Narula, S. K. Dhurandher, S. Misra, and I. Woungang, Security in Mobile Ad hoc Networks Using Soft Encryption and Trust Based Multipath Routing", Science Direct Computer Communication., Vol. 31, pp. 760–769, 2008.

[18] A. Abdul-Rahman and S. Hailes, "A Distributed Trust ModeL", Workshop on New Security Paradigms, Lansdale, Cambria, U.K., in Proceeding 1997, September 23–26, pp. 48–60, NSPW'97. ACM Press, New York, 1997

[19] A. A. Pirzada, A. Datta, and C. McDonald, "Propagating Trust in Ad-Hoc Networks for Reliable Routing", in Proc. 2004 Int. Workshop on Wireless Ad-Hoc Networks, May–Jun. 2004, pp. 58–62.

[20] S. Marti, T. J. Giulli, K. Lai and M. Baker "Mitigating Routing Misbehavior in Mobile Ad hoc Network", Mobile Computing and Networking, pp. 255- 265, 2000.

[21] S. Buchegger and J. Boudec, "Performance Analysis of the Confidant Protocol," Proc. International Symposium on Mobile Ad Hoc Networking and Computing, 2002.

[22] Y .Huang and W. Lee, "A Cooperative IDS for Ad hoc Network", Security of Ad Hoc and Sensor Networks, pp.135-145, ACM 2003.

[23] D. Barman Roy1 and R. Chaki" MADSN: Mobile Agent Based Detection of Selfish Node in MANET" International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 4, August 2011.

[24] Panthi N.K. et al. / (IJCSIT) International Journal of Computer Science and Information Technologies, "Securing Mobile Agent Using Dummy and Monitoring Mobile Agents" Vol. 1 (4) , pp. 208-211, 2010.