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

The APT Identification and Blocking through IDS in MANET

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

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

Abstract:**—**an advanced persistent threat (APT) is an attack on network in which an illegal someone gains access to a network and stays there is not detected for a long period of time. The purpose of an APT attack is to filch data rather than to cause damage to the network or organization. The APT is harmful for the network but in wireless network the servers and presence of administration is there for monitoring. The open network or without presence of administration, APT attack is flinch the whole network performance. This type of network is Mobile Ad hoc Network (MANET) that is creating the provisional network and also the link establishments are fluctuating and new topology are forming. In this research, proposed a security scheme is based on Intrusion Detection System (IDS). The attackers in MANET are easily damage the data and performing routing misbehavior. In MANET, uncooperative node is malicious node that functioning 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) has an ability to secure network from APT but difficult to design it. This research is applying the IDS to Malware like Virus Worm and Trojan horse multiple attackers. The IDS is measures the loss of APT and identified the attacker infection in dynamic network. The attackers or APT detection and prevention are possible on the basis of their attacker mechanism. There is no work is still proposed for securing MANET from unauthorized access through APT. The performance of HTTP, FTP over UDP and TCP, also measured performance through performance metrics like throughput and PDF.

***Keywords:* -** MANET, Attack, IDS, Routing, performance metrics, APT.

I. INTRODUCTION

The mobile Ad hoc Network (MANET) is the collection or group of mobile nodes established the temporary connection in between sender and receiver [1]. Due to the dynamic topology the changes of link breakage in this kind of network is more and also because of absence of administration attackers are easily modified or corrupt the network information [2]. It is well known that ad-hoc network is normally a kind of multi-hop, self-organized network, which is rapidly gaining popularity as a mode of communication, and provides facility to transmit or receive data among users or nodes in a common limited range of area. One feature of MANET is the communication between nodes established by multi-hop routing. If a couple nodes don't have connecting edge, they can hop by passing some edges and find a route path for indirect communication. Due to the dynamic nature, connections of all nodes are often changing. The Virus, Worms and Trojan horse are detection and prevention is only possible in this research. The effects of these arrackers are taken under the APT and applied the proposed security scheme on it. The APT is only attack on internet, that means real environment but in this simulation the scenario of attacker and effect of them in simulated and also evaluated the network performance. The security in MANET is a really a critical point of discussion. The MANET is vulnerable against attacks and the attackers are easily modified the original and normal performance of network by injecting the fake messages and dropping of valuable data of users. The attacks in MANET are classified in to two categories like active attack and passive attack [3]. The active attackers are very dangerous because they are actively participating in misbehavior activities for dumping the network performance at different layers of network. The examples of active attackers are well known Black hole attack, Wormhole attack, DoS attack and Sybil attack. The passive attackers are not all time actively misbehaving or performing malicious activities but they active only for some time (at ant instants means at any time) but watches network activities all time. The active attacker misbehavior is limited and it drop only small amount of data. Although these attackers are more dangerous than active attackers because their bury monitoring are maintaining the record of network which is harmful for future heavy disaster. The identification or detection of passive attackers is not very easy. The active attackers are not observing are whole network activities. They are behaves like a normal nodes but after successful connection establishment perform malicious activities. The encryption decryption security scheme and IDS (Intrusion Detection System) against passive and active attackers is identified or detect the malicious actions done by attackers. The IDS are of many types [4, 5] that are detecting the malicious activities of attacker and provide the secure communication in MANET. The attacker detection is not only necessary but prevention is also required. The prevention system is protect the network by disable the communication capability of attacker and this attacker malicious record is maintained some time to recognizes the attacker attacks in future is easily identified and prevent. APT Advanced Persistent Threads [6, 7] are among the most serious information security threats that organizations face today. A common goal of an APT is to steal intellectual property (IP) from the targeted organization, to gain access to sensitive 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. The Virus, Worms and Trojan are different attacks in network. These attackers has uses the different techniques for spreading the contagion in dynamic network. 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. The main aim of APT is not to only loss of data in network but also misplaces or modified the confidential information. In dynamic network the topology are frequently changes, which are the major cause of link breakage. The direct connection in between sender and receiver is rarely possible. The connections are created as multip-hop till the destination is not found. The routing protocol is playing an important role at network layer for data accepting and forwarding through each router or node. The data is sending by sender and accepted by receiver in this procedure routing strategy is very important part of communication [8, 9]. For connecting to destination and data delivery the routing protocol is necessary for routing the data in between sender to receiver. Every routing protocol has different routing strategy of connection establishment but has same method of select shortest path in between sender and receiver. The shortest path is decided on the basis of minimum hop count value in MANET. The classifications of routing protocols in MANET are as follows:-

A. Proactive Routing Protocol

The proactive routing protocols are also called as table driven routing protocol and these routing protocols are maintaining the routing information of each node that are participating in routing procedure. In Mobile Ad hoc network the topology in network is changes by that the overhead of maintain the information of each and every node is very difficult and required large amount of memory for storing routing information in network. In ad hoc network if the nodes are moves at slow speed then that protocol is suppose to be better for communication. The example of proactive routing protocol is DSDV routing protocol.

B. Proactive Routing Protocol

The proactive routing protocols are also called as table driven routing protocol and these routing protocols are maintaining the routing information of each node that are participating in routing procedure. In Mobile Ad hoc network the topology in network is changes by that the overhead of maintain the information of each and every node is very difficult and required large amount of memory for storing routing information in network. In ad hoc network if the nodes are moves at slow speed then that protocol is suppose to be better for communication. The example of proactive routing protocol is DSDV routing protocol.

C. Reactive Routing Protocol

The Reactive routing protocols are also called as on demand routing protocol and these routing protocols are maintaining the routing information on the basis of requirement of request receives by the neighbour. There is no routing information is stored of each node that are participating in routing procedure. In Mobile Ad hoc network the topology in network is changes by that the overhead of maintain the information of each and every node is not needed to maintained. In ad hoc network if the nodes are moves at random speed then that protocol is supposes to be better for communication. The example of reactive routing protocol is AODV routing protocol.

D. Hybrid Routing Protocol

Since proactive and reactive protocols each work best in oppositely different scenarios, hybrid method uses both. It is used to find a balance between both protocols. Proactive operations are restricted to small domain, whereas, reactive protocols are used for locating nodes outside those domains.

II. LITERATURE SURVEY

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 [10], 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 [11] 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 [12] the author's 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 [13] 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. Over the course of 2013, APT actors targeted many nations around the world, seeking national security secrets, research and development data and much more. Fire Eye threat [14] prevention platforms are normally placed behind traditional network defenses such as firewalls, next-generation firewalls, intrusion prevention systems (IPS), and anti-virus (AV) software. The Fire Eye appliances execute suspected malware in a virtual environment to observe and block malicious behavior. Most often, they analyze malicious activities that have succeeded in slipping past existing network defenses. Therefore they typically have extremely low false-positive alerts. Nonetheless, this report describes only attacks that fell within the Fire Eye field of vision in 2013. In other words, this research data encompasses only those attacks that met two criteria: (1) they struck Fire Eye customers. (2) Those Fire Eye customers agreed to share their attack metrics with Fire Eye. This report [15] analyzes unclassified data sets in an attempt to understand APT1's middle infrastructure: the system of hops, distribution points or relays, and the command and control (C2) servers that sit between APT1's victims and main C2 servers located overseas. To build that infrastructure, APT1 chose and exploited particular organizations to obfuscate communications while remaining in plain sight. This analysis, based on data from IP addresses known to be associated with APT1 and domain names provided by Mandiant, was conducted using a combination of System for Internet Level Knowledge (SiLK) tools, Microsoft Excel, and custom Python scripts. The study detailed in this report can be replicated easily using available sources and tools. By combining key unclassified information, the authors successfully described a large, malicious network used to steal important information.

III. PROBLEM STATEMENT

The attack in network is degrades the performance of protocols and also corrupt the confidential information or disclose confidential information. In wireless network the sender and receiver information is controlled by base station or servers. But in Mobile Ad hoc Network it is not possible to apply the any base station control on it. Now one more problem in MANET is odes are continuously moves with a different mobility speed. The APT is really a harmful attacker for this kind of network. The Malwares i.e. considered in this research is really a killer of data in the network or disclose the confidential information. The Virus, Worms and Trojan horse are combined to attack on MANET. The problem is faces due to APT in MANET are as follows:-

1. The attackers attack behaviour is different due to that single security scheme is not possible it is necessary to apply the security by identified the infection spreading mechanism or at network do routing misbehaviour.
2. The routing performance of network is affected because of degradation in throughput and routing overhead.
3. The application layer protocol performance is also affected because of minimizes the packets receiving at destination end.
4. Attackers are infuses the abnormal behaviour because of that heavy loss on data is observe.

IV. PROPOSED WORK

The proposed Intrusion Detection System (IDS) is applied on APT to stop the malicious activities in dynamic network. In this network the security against APT is possible by applying IDS security scheme. The behaviour of Virus, Worms and Trojan horse is first identified by attacker and this behaviour is helps to IDS to identified and block the attacker through previous and current information available. If the information is matched then no further examination is necessary if information is different than evaluated the infection ratio of attackers that confirm the attacker existence. In this algorithm we detect and prevent from worm, virus and Trojan using us say Multi-attack intrusion prevention system for APT in MANET. In this section define the algorithm in step by step process.

A. Algorithm Step for APT attack intrusion Prevention System

```
    Algorithm: Compute IDS
    Input:
N: set of mobile nodes
            S: set of Sender Nodes
            I: set of intermediate nodes
            R: Set of Receiver Nodes
            IDS node: p ϵ N  ← set of preventer node
            A_p: suspected node
            a ϵ N: set of attacker nodes whose spread worm, virus, Trojan
    Output:
        Attacker node information, PDR, receives and sends information
    S← execute-route(S, R, IDS)
    While (N =in range) do
        I ← receive routing packets
        For each I in range, p watches the I and set A_p
        Call_IDS (I, packet)
        While I ≠ R do
                Calculate PDR of I: (forward/receives)
        If (I== R) then
                Send Ack to S node
                Call data-pkt ()
        Else
                R not in zone
                End if
        End do
    End do
    IPS (node, packet_type)
        If (I update data of S node)
        Check updates data by I
        If (update is True && receiver ID is modified)
        I ϵ a
        Identifies (infected data value, node number, symptoms)
        End if
        End if
        While (symptoms! = normal) Do
                If (symptoms == 'Worm')
                Modified node number, new symptoms
                Analyze behaviour
                Trace time of data update
                Else if (symptoms == Virus)
                Identifies attacker a
                Abnormal data set identification
                Number of node infected
                Else if (symptoms == Trojan)
                a shows normal node
                Modified the packets and drop
                End if
        End do
    Prevention-manager IDS (attack type, abnormal-table)
        Analyze attack type with abnormal table
        Send normal treat msg to a
```

```
If (profiles == normal-profile)
a ϵ normal profile node
Attack removes
Else
Block the node with symptoms
End if
```

IPS Broadcast attacker node info and its symptoms to all connected node New path established for communication Analyse the new network behaviour Calculate performance of the network.

V. SIMULATION & RESULT DESCRIPTION

The simulation of all scenarios is simulated in NS-2 simulator. The NS-2.31 (Network Simulator version 2.31) is used for simulating the APT affect in dynamic network. The work in APT with MANET is done in first time. This simulator is open source code and due to that the modification in internal modules are possible. It is discrete event simulator (timing of events is maintained in a scheduler). This simulator is developed by Start 1989 as a variant of REAL (network simulator for studying the dynamic behavior of flow and congestion control schemes in packet-switched data networks) after 1995, Funding from DARPA through many projects (VINT project at LBL, Xerox PARC, UCB, and USC/ISI. SAMAN and NSF with CONSER). Table 1 are represents the following simulation parameters to make the scenario of routing protocols. The detailed simulation model is based on network simulator-2 is used in the evaluation.

Table 1 Simulation parameters will uses for simulation

Simulator Used	NS-2.31
Number of nodes	50
Radio Range (meters)	250m
Attacker	APT
Routing Security	IDS
Dimension of simulated area	800m×600m
Routing Protocol	AODV
Simulation time	100 sec.
Traffic type (TCP & UDP)	FTP, CBR (2pkts/s)
Packet size	1024 bytes
Number of traffic connections	4, 2
Node movement at MAX Speed	random (20 m/s)

B. Performance Metrics

It's computed the following metrics for after the simulation of Sybil attacker and proposed IDS. Packet overhead: - The number of transmitted routing packets; for example, a HELLO or RREP and RREQ message sends by all senders in network. Attacker Loss Percentage: - This metrics is calculated the data packets that is drop by attacker in network. Detection Accuracy: - To identify the attacker loss malicious actions, in uses this metrics in order to determine the detection accuracy of APT i.e. Virus, Worms and Trojan horse. HTTP Receiving Analysis: - The number of packets receiving at destination in case of APT and IDS is evaluated through this performance. Here the performance of HTTP over UDP is measured. The results are evaluated in three scenarios first is normal performance of network, second is the network is in under the APT and the third is applied the proposed IDS on APT.

C. HTTP Over UDP Packets Received Analysis

The attacker in MANET is really loss or discloses the private data. The APT is not only harmful for the wireless network but in wireless network it is possible to detect the APT attack misbehavior through base stations and servers. The HTTP protocol is the application layer protocol. In this graph the performance of HTTP protocol over end to end protocol FTP is measured, only in case of packets receiving in network. The packet loss or information discloser because of Virus, Worms and Trojan is really more by that negligible receiving is count. However the performance of proposed IDS is equivalent to normal network performance that shows the effective performance of proposed IDS in dynamic network.

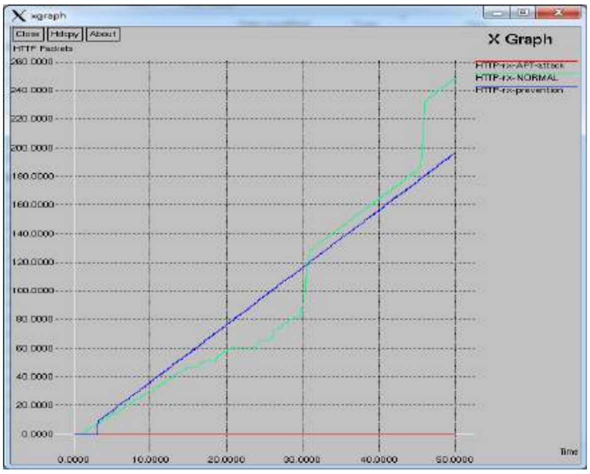

Fig.1 HTTP Protocol Receiving Data Analysis

D. APT Loss Analysis in MANET

The nodes in MANET are continuously moves and try to establish the connection between the neighbors. If the nodes movement is fast in that case the strong link establishment is not possible. The Malware nodes in network are continuously moves and their reorganization is easily not possible, if they continuously moves and also due to Virus, Worms and Trojan horse presence network performance is almost counted negligible. In this graph the APT loss in term of Virus, Worms and Malware are detected and observe that the 45 % data is loss and modified by the Worms and Trojan. The worm hole is initiated from the start of simulation and their effect is only maximum 12 % up to the time 40 seconds but after that the Virus and Worms are affected the network performance.

E. PDR Performance Analysis

In network the Malwares are strike to identify the network actual activities. That means the APT is aim is not to drop the data in the network but their aim is to loss, modified and discloses the data to unauthorized users. The APT is harmful because it contains the property of multiple attackers and these attackers are performing their duties strictly. The PDR performance of normal network is and IDS presence against APT is about 90 % up to end of simulation but in presence of attacker the PDR performance is only evaluated up to 20 seconds. The malicious activities of APT in routing misbehavior in the network are all most negligible due to presence of IDS. The proposed IDS is provides the secure routing in between source to destination in the dynamic network.

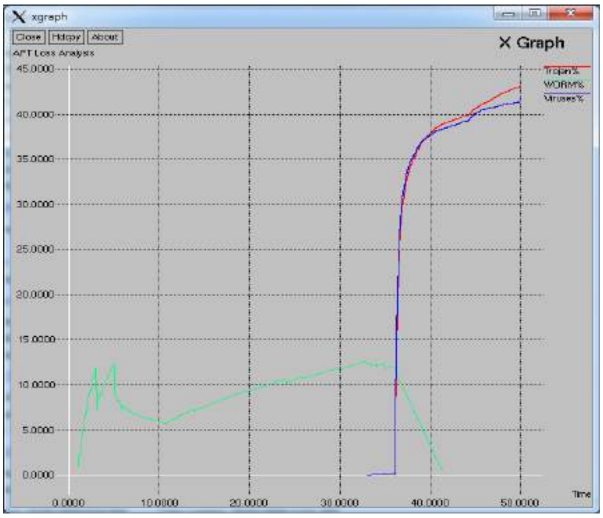

Fig.2 APT Loss Percentage in Network

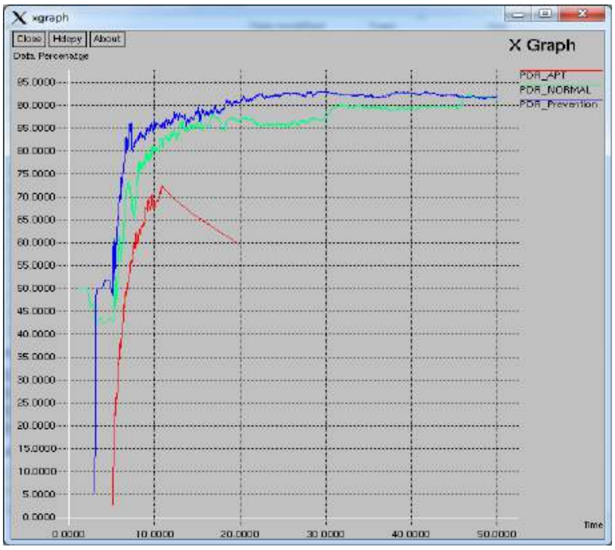

Fig.3 PDR Analysis

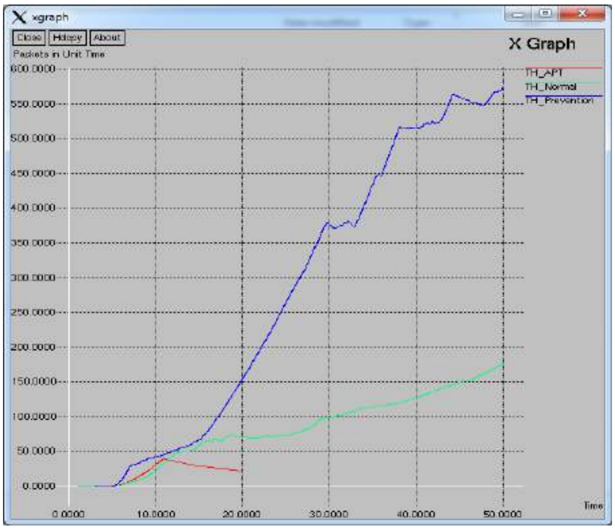

Fig.4 Throughput Analysis

F. Throughput Performance Analysis

The Virus, Worms and Trojan horse are the effective Malwares and their combined effect is definitely possible to obliterate network normal activities. The routing misbehavior is easily possible in open MANET and their reorganization is only possible, if the receiver is not received the proper data. In throughput performance the data packets are counted in per second at destination. The better throughput performance are shows the better network performance. The throughput performance of APT is really blatant but the attacker symptoms are identified by the secure IDS and improve the through performance. The attackers nodes are completely blocked by IDS by that number of nodes are minimized but due to avoid the attacker presence it is necessary to choose another path and this new path is better than the previous. That's why the throughput performance is high.

G. FTP Over TCP Packets Analysis

The APT is not attack directly on network but it is first attack on particular host or node in network and their infection is spread in network. The FTP protocol is the application layer protocol over end to end TCP protocol. Here the data receiving is observed in *congestion windows*. The data receiving in attacker is also most negligible bit the proposed IDS are recovers the attack and provides secure routing in presence of attacker. The IDS has heist congestion window of packet size of 34 bytes. The performance of normal network is not reaches more than 22 seconds.

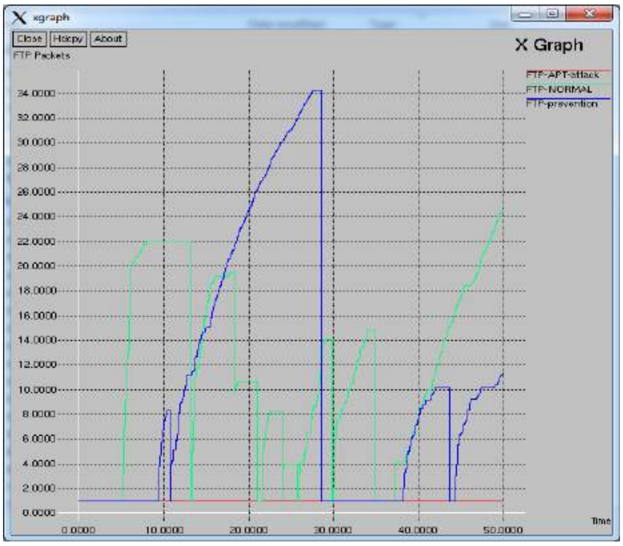

Fig.1 FTP over TCP Analysis

VI. CONCLUSION & FUTURE WORK

Advance Persistent Threat (APT) is among the most genuine data security threat that associations confront today. A typical objective of an APT is to take intellectual assets from the focused organizations or associations, to access responsive customer data. The APT is the serious problem in MANET it will not damage the whole data but the data confidentiality is lose by attacker. The APT is attack on network it means that the routing performance of attack is also modified or affected. The APT or Malware i.e. Virus, Worms and Trojan horse is loss or degrades the use full information and performance of network. The effect of these attackers are dangerous and everyone is attack mechanism is different. In open or decentralized network called Mobile Ad hoc Network (MANET), providing security is a critical issue. In this research, the proposed secure IDS provide the security against APT and the attackers or Malware in network is Virus, Worms and Trojan horse. The malicious functioning and loss of data is degrades the whole network performance. The mainstream of active malware threats are usually loss the data or lose the confidential information. The proposed IDS is applied on APT or Malware and identified that the infection through Virus, Worms and Malware are completely removed by attacker in network. The infection through Malware is not detected in presence of IDS security scheme in MANET. The main problem is APT has the combination of different attacks the proposed IDS is really effective that recognized the symptom of attacker through spurious type malicious entries in network, that is not recognized as normal routing of data in network. The APT has a capability to block the performances and IDS against provides the secure communication to mobile nodes in MANET. The proposed research is blocks the APT Malware detection and provides secure communication in MANET. In future we also combined the effect of MANET attackers like black hole attack or wormhole attack with APT and apply the proposed IDS on it and also try to modify IDS by including GPS (Global Positioning System) to identify the location of attacker in dynamic network.

REFERENCES

[1]. G. P. Papadimitratos and Z. Haas, "Handbook of Ad Hoc Wireless Networks", Chapter Securing Mobile Ad hoc Networks. CRC Press, 2002.

[2]. Q. Guan, F. R. Yu, S. Jiang, V. Leung, and H. Mehrvar, “Topology Control in Mobile Ad Hoc Networks with Cooperative Communications,” IEEE Wireless Communication., Vol. 19, No. 2, pp. 74–79, Apr. 2012.

[3]. Mohammad O. Pervaiz, Mihaela Cardei, and Jie Wu, "Routing Security in Ad Hoc Wireless Networks", Mohammad O. Pervaiz, Mihaela Cardei, and Jie Wu Springer pp.1-32, 2005

[4]. B. Sun, L. Osborne, Y. Xiao, and S. Guizani, "Intrusion Detection Techniques in Mobile Ad Hoc and Wireless Sensor Networks," IEEE Wireless Communications Magazine, special issue on Security in Wireless Mobile Ad Hoc and Sensor Networks, Vol.14, No.5, pp. 56-63, October 2007.

[5]. Adnan Nadeem and Michael P. Howarth, “A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks" IEEE Communications Surveys & Tutorials, Accepted for Publication, pp.1-19, 2013.

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

[7]. 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

[8]. Elizabeth M. Royer, Chai-Keong Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks", IEEE Personal Communications, Vol. 6, No. 2, pp. 46-55, April 1999.

[9]. Anuj K. Gupta, Harsh Sadawarti, and Anil K. Verma, "Review of Various Routing Protocols for MANETs", International Journal of Information and Electronics Engineering, Vol. 1, No. 3, pp. 251-259, November 2011.

[10]. 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.

[11]. 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.

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

[13]. 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.

[14]. Fire eye Advanced Threat Report, 2013, Available on link www.fireeye.com.

[15]. Deana Shick Angela Horneman "Investigating Advanced Persistent Threat 1 (APT1)", A Technical Report May 2014, Copyright 2014 Carnegie Mellon University http://www.isi.edu/nsnam/ns/edu/index.html.