International Journal For Technological Research In Engineering
Volume 3, Issue 8, April-2016 *ISSN (Online): 2347 - 4718*

ELIMINATION AND DETECTION OF TROJAN ATTACK IN WSN AND MANET

Pankaj Gupta[1], Yogender Pal[2]
[1]M.Tech(Computer Science), [2]Assistant Professor M.Tech(CS), Manav Bharti University

ABSTRACT: Wireless ad-hoc networks monitor dynamic environments that change rapidly over time. This dynamic behavior is either caused by external factors or initiated by the system designers themselves. To adapt to such conditions, ad-hoc networks often adopt machine learning techniques to eliminate the need for unnecessary redesign. Machine learning also inspires many practical solutions that maximize resource utilization and prolong the lifespan of the network. In this paper, we present an extensive literature review over the period 2002-2014 of machine learning methods that were used to address common issues in wireless ad-hoc networks (WSNs). The advantages and disadvantages of each proposed algorithm are evaluated against the corresponding problem. We also provide a comparative guide to aid WSN designers in developing suitable machine learning solutions for their specific application challenges. We present an overview of embedded network applications and discuss requirements arising from this analysis. Furthermore, we discuss selected in-network processing techniques and point out the analogy between Hopfield neural and back propagation networks. In the following neural networks are introduced in the ad-hoc network context. We describe the motivation and the practical case for neural networks in the ad-hoc networks context, and evaluate early results achieved with our test implementation. We argue that there is a high potential with these paradigms which promise a strong impact on the future research, especially if applied as a hybrid technology. We are implementing this for WNS for finding Collision in Ad-hoc network and also try to find out the throughput value of the data that is transmitted over the ad-hoc network. We simulated the Trojan attack in wireless ad-hoc networks and evaluated its damage in the network. We made our simulations using MATLAB- 10 simulation program that consists of the collection of all network protocols to simulate many of the existing network topologies. Even though MATLAB- 10 contains wireless ad-hoc routing protocols, it does not have any modules to simulate malicious protocols. Thus, to simulate Trojan attacks, we first added a new Trojan protocol into the MATLAB - 10. We started our study by writing a new AODV protocol using MAT files, to simulate the Trojan attack. Having implemented a new routing protocol which simulates the Trojan we performed tests on different topologies to compare the network performance with and without Trojans in the network. As expected, the throughput in the network was deteriorated considerably in the presence of a Trojan. Afterwards, we proposed an IDS solution to eliminate the Trojan effects in the AODV network. We implemented the solution into the MATLAB-10.And evaluated the results as we did in Trojan implementation. As a result, our solution is eliminated the Trojan effect with 24-38% success.

Keywords: Trojan, WSN, MANET, Collosion, Dynamics, AODV protocol.

I. INTRODUCTION

Wireless ad-hoc networks are composed of autonomous nodes that are self- managed without any infrastructure. In this way, ad-hoc networks have a dynamic topology such that nodes can easily join or leave the network at any time. They have many potential applications, especially, in military and rescue areas such as connecting soldiers on the battlefield or establishing a new network in place of a network which collapsed after a disaster like an earthquake. Ad-hoc networks are suitable for areas where it is not possible to set up a fixed infrastructure. Since the nodes communicate with each other without an infrastructure, they provide the connectivity by forwarding packets over themselves. To support this connectivity, nodes use some routing protocols such as AODV (Ad-hoc On-Demand Distance Vector), DSR (Dynamic Source Routing) and DSDV (Destination-Sequenced Distance-Vector). Besides acting as a host, each node also acts as a router to discover a path and forward packets to the correct node in the network.

As wireless ad-hoc networks lack an infrastructure, they are exposed to a lot of attacks. One of these attacks is the Trojan attack. In the Trojan attack, a malicious node absorbs all data packets in itself, similar to a hole which sucks in everything in. In this way, all packets in the network are dropped. A malicious node dropping all the traffic in the network makes use of the vulnerabilities of the route discovery packets of the on demand protocols, such as AODV. In route discovery process of AODV protocol, intermediate nodes are responsible to find a fresh path to the destination, sending discovery packets to the neighbor nodes. Malicious nodes do not use this process and instead, they immediately respond to the source node with false information as though it has fresh enough path to the destination. Therefore source node sends its data packets via the malicious node to the destination assuming it is a true path. Trojan attack may occur due to a malicious node which is deliberately misbehaving, as well as a damaged node interface. In any case, nodes in the network will constantly try to find a route for the destination, which makes the node consume its battery in addition to losing packets.

1.2 Wireless Networks

Wireless communication is used to transfer data among users without a wired infrastructure. Using electromagnetic waves, mobile users transmit and receive data over the air. Wireless communication spreads from home RF to satellites, from cellular phones to walkie-talkies. Its mobility, simplicity and cost saving installation advantages make the wireless communication more popular, especially in recent decades Increasing user mobility needs and developments in the use of laptop computers and PDA's is one of the main reasons of the popularity of wireless networks.

1.2.1. Convenience Offered by Wireless Networks Mobility

This is one of the obvious advantages of the wireless networks. Mobile users can connect to the existing networks while roaming freely and enjoying independence. Simplicity we can translate simplicity into rapid development. It is easy to install a wireless infrastructure, compared to a wired network. Flexibility Wireless network coverage area can reach where wire cannot go. It is very useful for moving vehicles or for the places where running cable is not possible like historical buildings.

1.2.2. Types of Networks

According to coverage area, three type of wireless interconnection have been defined. Personal Area Networks (PANs), Local Area Networks (LANs) and Wide Area Networks (WANs).

A. Personal Area Networks (PAN)

PAN is a computer network used for communication among computer devices (including telephones, PDAs, etc.) close to one person. Typical PAN networks are Bluetooth, Sensor networks and zigbees. The Standards Board of the IEEE approved the standard 802.15, as MAC and PHY Specifications for Wireless PANs (WPANs).

B. Local Area Networks (LAN)

In this type of network, devices are communicating with each other in a local coverage area that can be a building or a campus. Wireless LANs (WLANs) are alternatives of conventional wired LANs. In a wired network nodes are communicating over physical environments such as cables. On the other hand, in a WLAN nodes use air as the medium. WLANs are standardized by Institute of Electrical and Electronics Engineers (IEEE).

C. Wide Area Networks (WAN)

WANs spread a relatively larger geographical area. Typically a WAN includes more than one LANs. 2G and 3G Mobile Cellular Networks, Satellite Systems and Paging Networks are examples of Wireless WANs (WWANs) Figure 1 shows the ways in which different types of wireless networks and hardware may be used together to provide the best performance and mobility.

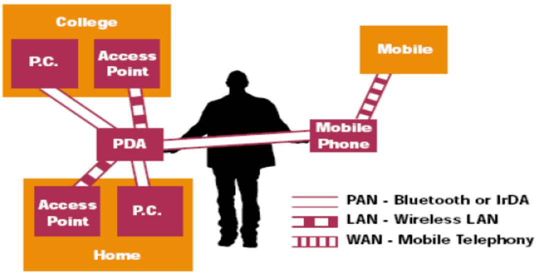


Figure 1 - Wireless uses in differing environments

Figure 1 shows that anybody who uses a PDA (equally a laptop) can access to the PCs in a wireless infrastructure using Bluetooth or WLAN technology while connecting with mobile phone over GSM. Actually Figure 1 indicates how wireless networks support mobility, simplicity and flexibility.

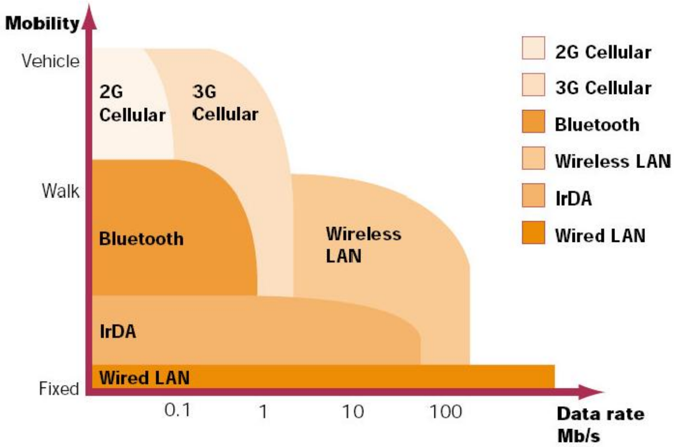


Figure 2 - Data rates and mobility for communication types

Figure 2 shows various types of wireless communication and their data rates and mobility. From this it can be seen that there is a balance to be struck between performance and mobility.

1.2.3. Wireless Local Area Networks (WLAN)

WLANs are alternative of conventional LANs that connect nodes in wired environments. WLANs transmit information over wireless medium instead of wire. A Wireless Local Area Networks (WLAN) is a shared medium communication network that broadcast information over wireless links to be received by all stations (e.g. computing devices). WLANs are used mainly to connect to the Internet. Wireless internet access points are known as "hot spots" and are already available in coffeehouse and other public places such as airports, stations and hotels. Thanks to these benefits, WLANs have gained significant popularity among mobile users to access real-time information. Actually WLANs are implemented in mobile devices such as laptops, PDAs etc. to communicate with each other without using wired Ethernet (IEEE 802.3). In a WLAN, instead of wired Ethernet protocol, IEEE 802.3, wireless Ethernet protocol, IEEE 802.11 is used.

1.2.4. IEEE 802.11 Standards, Specifications and Technologies

IEEE 802.11 is a member of the IEEE 802 protocol family, which defines specifications of Local Area Network (LAN) technologies. IEEE 802 specifications are focused on two lowest layers of the OSI model, the MAC and the physical (PHY) component that incorporate each other. In the IEEE 802 series, individual specifications are determined after the point. 802.3, for example design Carrier Sense Multiple Access network with Collision Detection (CSMA/CD) and 802.5 is the Token-Ring specification. Figure 3 shows the various components of the 802 family and their relation with the ISO models.

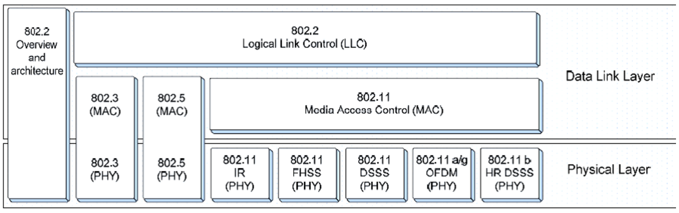


Figure 3 – IEEE 802 family and relation with the ISO models

In Figure 3, there are four modulation techniques in the physical layer and four specifications in 802.11 families. Table 1 compares the 802.11 family standards.

IEEE Standards	Speed	Frequency	Interface
802.11	Up to 2 Mbps	2.4 GHz	IR / FHSS / DSSS
802.11a	Up to 54 Mbps	5 GHz	OFDM
802.11b	Up to 11 Mbps	2.4 GHz	HR-DSSS
802.11g	Up to 54 Mbps	2.4 GHz	OFDM

Table 1 - Comparison of 802.11 standards

IEEE 802.11 standards / specifications / technologies referred to as Wi-Fi (Wireless Fidelity) that is also a trademark of the Wi-Fi Alliance, a nonprofit organization originally formed as WECA (Wireless Ethernet Compatibility Alliance).

1.2.5. WLAN Modes

If minimum two stations in a BSA communicate with each other, they are members of the BSS. The 802.11 standard has two BSS modes. These are ad-hoc and infrastructure networks. These two networks are illustrated in Figure 5 and Figure 6.

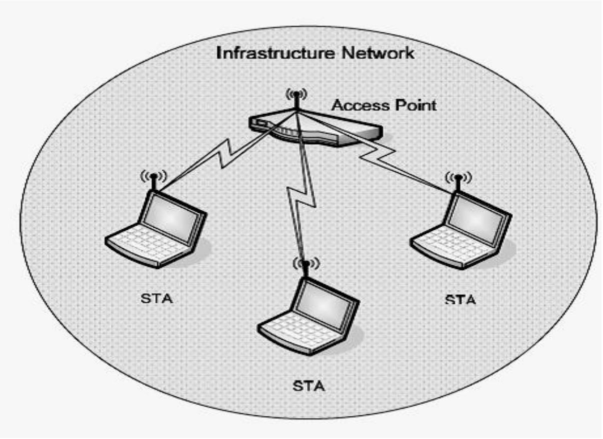


Figure 5 - Infrastructure Network

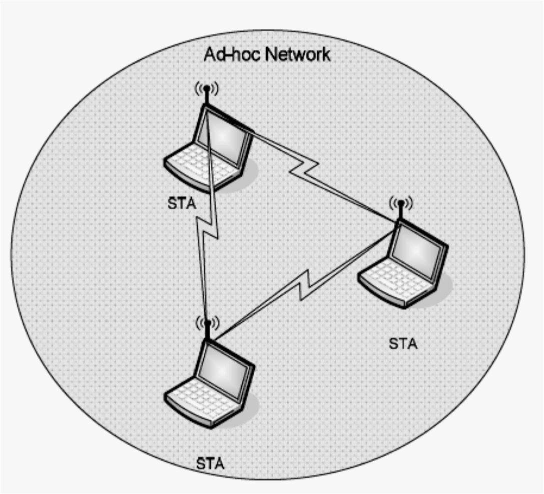


Figure 6 - Ad-hoc Network

1.2.6. Routing In MANETs

MANETs have special limitation and properties such as limited bandwidth and power, highly dynamic topology, high error rates etc., explained in the preceding sections. Moreover, compared to infrastructure based networks, in a MANET, all nodes are mobile and can be connected dynamically in an arbitrary manner. Nodes of MANET behave as router and take part in discovery and maintenance to establish a reliable route of each other. Therefore, routing protocols for wired networks cannot be directly used in wireless networks and numerous protocols have been developed for MANETs. These routing protocols are divided into two categories based on management of routing tables. These categories are Table Driven Routing Protocols and On-Demand Routing Protocols, shown in the Table 2 and they are explained below:

MANET ROUTING PROTOCOLS	
Table Driven Routing Protocols	**On-Demand Routing Protocols**
Destination-Sequenced Distance Vector Routing Protocol (DSDV)	Ad-Hoc On-Demand Distance Vector Routing (AODV)
Wireless Routing Protocol (WRP)	Cluster based Routing Protocols (CBRP)
Global State Routing (GSR)	Dynamic Source Routing Protocol (DSRP)
Fisheye State Routing (FSR)	Temporally Ordered Routing Algorithm (TORA)
Hierarchical State Routing (HSR)	Associativity Based Routing (ABR)
Zone-based Hierarchical Link State Routing Protocol (ZHLS)	Signal Stability Routing (SSR)
Clusterhead Gateway Switch Routing Protocol (CGSR)	

Table 2 – Classification of MANET routing protocols

1.2.7. Security Issues for MANETs

Vulnerabilities of operating systems and upper layer applications that belong to user programs such as databases, browsers or client-server applications are not considered as a security issue for ad-hoc networks. General attack types are the threats against the routing layer of the ad-hoc networks; such as physical, MAC and network layer which is the most important function of wireless ad-hoc network for the routing mechanism, orienting the packets after a route discovery process. Other vulnerabilities are application security, network security, database security which are studied in different works which are not explained in detail here.

Attacks to the wireless ad-hoc network in the networking layer usually have two purposes: not forwarding packets or adding and changing some parameters of routing messages; such as sequence number and IP addresses. These will be detailed in the subsequent sections.

Using one of the key mechanisms such as cryptography or authentication, or both in a network, serves as a preventive approach and can be employed against ‘attackers’. However, these mechanisms protect the network against attacks that come from outside, malicious ‘insiders’ which use one of the critical keys can also threaten the security. For instance, in a battle field where ad-hoc networks are used, even if keys are protected by temper proof hardware that are used in the vehicles in the network, it is difficult to say that these vehicles exhibit the same behavior if the enemy captures them.

On the other hand, a node may undeliberately misbehave as if it is damaged. A node with a failed battery which is unable to perform network operations may be perceived as an attack. Another malicious behavior of the nodes is selfishness. Selfish nodes refrain from consuming its resources; such as battery, by not participating in network operations. Therefore; failed and selfish nodes also affect the network performance as they do not correctly process network packets, such as in routing mechanism.

We should, therefore ensure that everything is correctly working in the network to support overall security and know how an insider is able to attack the wireless ad-hoc network. Wireless ad-hoc networks should be protected with an intrusion detection system that can understand the possible actions of attackers and can produce a solution against these attacks.

II. LITERATURE SURVEY

Sanjeet1, Asst Prof. Sonia Rani2 proposed the Trojan attack in wireless ad-hoc networks and evaluated its damage in the network. We made our simulations using MATLAB- 10 simulation program that consists of the collection of all network protocols to simulate many of the existing network topologies. Even though MATLAB- 10 contains wireless ad-hoc routing protocols, it does not have any modules to simulate malicious protocols. Thus, to simulate Trojan attacks, we first added a new Trojan protocol into the MATLAB- 10. We started our study by writing a new AODV protocol using MAT files, to simulate the Trojan attack. Wireless ad-hoc networks are composed of autonomous nodes that are self- managed without any infrastructure. In this way, ad-hoc networks have a dynamic topology such that nodes can easily join or leave the network at any time. They have many potential applications, especially, in military and rescue areas such as connecting soldiers on the battlefield or establishing a new network in place of a network which collapsed after a disaster like an earthquake. Ad-hoc networks are suitable for areas where it is not possible to set up a fixed infrastructure. Since the nodes communicate with each other without an infrastructure, they provide the connectivity by forwarding packets over themselves. Wireless communication is used to transfer data among users without a wired infrastructure. Using electromagnetic waves, mobile users transmit and receive data over the air. Wireless communication spreads from home RF to satellites, from cellular phones to walkie-talkies. Its mobility, simplicity and cost saving installation advantages make the wireless communication more popular, especially in recent decades Increasing user mobility needs and developments in the use of laptop computers and PDA’s is one of the main reasons of the popularity of wireless networks.

Sureka.N1, Prof. S. Chandra Sekaran proposed resource depletion attacks at the routing protocol layer, which permanently disable networks by quickly draining nodes’ battery power. These “Vampire” attacks are not specific to any specific protocol, but rather rely on the properties of many popular classes of routing protocols. We discuss methods to mitigate these types of attacks, including a new proof-of-concept protocol that provably bounds the damage caused by Vampires during the packet forwarding phase. The wireless Adhoc sensor network and routing data in them is vulnumarable to certain attacks. So we must ensure a secure and authenticated data transmission process. There are a lot of protocols developed to protect from DOS attack, but it is not completely possible. One such DOS attack is Vampire attack draining of node life from wireless adhoc sensor networks. Adhoc wireless sensor networks (WSNs) promise exciting new applications in the near future, such as ubiquitous on-demand computing power, continuous connectivity, and instantly deployable communication for military and first responders. Such networks already monitor environmental conditions, factory performance, and troop deployment, to name a few applications.

Harsha.N1, Rashmi.S proposed an approach to detect and prevent the vampire attack in MANET. Ad-hoc low-power wireless networks are the most promising research direction in sensing and pervasive computing. Prior security work in this area has focused primarily on denial of service at the routing or medium access control levels. Earlier, the resource depletion attacks are considered only as a routing problem, very recently these are classified in to a new group called “vampire attacks”. Vampire attacks are not protocol-specific, in that they do not rely on design properties or implementation faults of particular routing protocols, but rather exploit general properties of protocol classes such as link-state, distance vector, source routing, and geographic and beacon routing .It is clear that all examined protocols are susceptible to Vampire attacks, which are devastating, difficult to detect, and are easy to carry out using as few as one malicious insider sending only protocol compliant messages. In the worst case, a single Vampire can increase network-wide energy usage by a factor of O (N), where N in the number of network nodes.

Sumit Agrawal, Shilpa Jaiswal proposed a Secure Ad-hoc On-Demand Distance Vector routing protocol (SAODV) to endeavor our all efforts into a common place. So the emphasis is to develop a scheme for the measure of these network worms and blackhole attacks to eliminate occurrences of communication hazards from intermediate and surrounding threads. the full study to eliminate thread of black hole attacks in MANET”. We also address to the solution against the threat of black hole attack in MANET. In Black Hole Attack a malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept. So to rectify the possibility of occurrence of black hole attack we are proposing a technique to identify attack and a solution to discover a safe route for secure transmission. The need of wireless network is to enforce participating nodes to forward packets to other nodes to foster secure and reliable communication. Although there are presence of vulnerable nodes that can be associated with malicious nodes and can harm networks. The varieties of these malicious nodes are vulnerable to nodes which are either compromised or falsely guided by vulnerable nodes. Malicious nodes can easily tamper the participating nodes in the networks. In mobile ad hoc network these attacks shown their significance in the terms of network worms which can attack, alter or modify the root definitions of network across all administrative and participating domains.

Saritha Reddy Venna1, Ramesh Babu Inampudi proposed vulnerabilities and various kinds of security attacks in MANETs The recent and rapid advancements in the technology and the distinct features of MANETs have made the use of MANETs more prevalent. With the ever increasing applications, the weakness of these networks against a variety of attacks has been unveiled. MANETs doesn’t have clear and efficient mechanisms to detect or prevent the attacks, so attacker node can easily interrupt and destroy the whole system or may take control over the information being transmitted in the network. Attackers introduce various kinds of attacks and every attack has its own degree of impact on the network. Security is a major concern in MANETs because of its intrinsic vulnerabilities. Each mobile node can work either as a host or as a router. There is no necessity of fixed infrastructure and these mobile nodes organize themselves in an arbitrary fashion to form a temporary network with dynamically changing topology. Nodes within each other’s wireless transmission ranges can communicate directly but nodes outside each other’s rangehave to depend on neighbouring nodes to relay messages.

Guozhu Meng, Yang Liu, Jie Zhang, Alexander Pokluda, Raouf Boutaba proposed different mechanisms of collaboration and defense in collaborative security. We systematically investigate numerous use cases of collaborative security by covering six types of security systems. Aspects of these systems are thoroughly studied, including their technologies, standards, frameworks, strengths and weaknesses.We then present a comprehensive study with respect to their analysis target, timeliness of analysis, architecture, network infrastructure, initiative, shared information and interoperability. We highlight five important topics in collaborative security, and identify challenges and possible directions for future research. Our work contributes the following to the existing research on collaborative security with the goal of helping to make collaborative security systems more resilient and efficient. Security is oftentimes centrally managed. An alternative trend of using collaboration in order to improve security has gained momentum over the past few years. Collaborative security is an abstract concept that applies to a wide variety of systems, and has been used to solve security issues inherent in distributed environments. Thus far, collaboration has been used in many domains such as intrusion detection, spam filtering, botnet resistance, and vulnerability detection.

K.Sivakumar1, P.Murugapriya2 proposed optimal energy boost-up protocol (OEBP) analyzes the routing table and verify the attacks which permanently disable networks by quickly draining nodes’ battery power. These “Vampire” attacks are not specific to any specific protocol, but rather rely on the properties of many popular classes of routing protocols. This enhanced work increases the Quality of service in the network and it will regulates all the nodes activity. AD hoc wireless sensor networks (WSNs) promise exciting new applications in the near future, such as ubiquitous on-demand computing power, continuous connectivity, and instantly deployable communication for military and first responders. Such networks already monitor environmental conditions, factory performance, and troop deployment, to name a few applications. Vampire attacks are not protocol-specific, in that they do not rely on design properties or implementation faults of particular routing protocols, but rather exploit general properties of protocol classes such as link-state, distance vector, source routing, and geographic and beacon routing..

Manju.V.C. proposed the security aspects of wireless sensor networks. Here we have done a study on the current security threats, countermeasures, link layer protocols and cryptographic communication schemes. Efficient design and implementation of wireless sensor networks have become a hot area of research in recent years due to the vast potential of the sensor networks to enable application that connect the physical world to the virtual world. Wireless platforms are becoming less expensive and more powerful, enabling the promise of widespread use for everything from health monitoring to military sensing. While wireless sensor networks are quite useful in many applications it appears that they are more vulnerable to attacks than wired networks. So there is a need to have better wireless sensor security. A wireless sensor network consists of spatially distributed autonomous sensors to cooperatively monitor physical or environmental conditions such as pressure, temperature, sound, vibration motion or pollutants. WSN is used to locate not only the objects whose area of location is known but also the objects whose location is anticipated to be around a certain domain. Each node in a sensor network is typically equipped with a radio receiver, a small micro controller, energy source usually a battery. Sensor networks can be used for target tracking, system control and chemical and biological detection. In military application's sensor, networks can enable soldiers to see around corners and to detect chemical and biological weapons long before they get close enough to cause harm them.

Ambili M A1, Biju Balakrishnan proposed how routing protocols,affect from attack even those designed to be secure, lack protection from these attacks, which we call Vampire attacks, which permanently disable networks by quickly draining nodes’battery power.These“Vampire”attacks are not specific to any specific protocol which are devastating, difficult to detect,and are easy to carryout using as few as one malicious insider sending only protocol compliant messages.We propose an energy constraintintrusion detection technique to detect there source draining attack. Wireless Sensor Networks came into prominence around the start of this millennium motivated by the omni present scenario of small-sized sensors with limited power deployed in large numbers over an area to monitor different phenomenon.The applications ofWSNwererapidlyemerging& havebeen increasingly diverse, including medical monitoring, homeland security, industrial automation, military application etc. This highlights the need for security as sensor nodes are highly susceptible to many kinds of attacks.Some attacks called Resource consumption attacks that are difficult to detect will deplete the nodes energy and thus permanently disable the network.The sole motivation for research in WSN has been to provide security and to maximize the lifetime of the network, where network lifetime is typically measured from the instant of deployment to the point when one of the nodes has expended its limited power source and becomes in-operational–commonly referred as a first node failure.

Varalatchoumy.M, Sowmya H.K. Kohilambal R, proposed an overview of attacks according to the protocol layers, and to security attributes and mechanisms. Counter measures for these attacks are presented following the order of the protocol layers. An ad hoc network is a collection of wireless mobile nodes that forms a temporary network without any centralized administration. In such an environment, it may be necessary for one mobile node to enlist other hosts in forwarding a packet to its destination due to the limited transmission range of wireless network interfaces. Due to open medium, dynamic topology, distributed cooperation, and constrained capabilities ad hoc networks are more vulnerable to many types of attacks compared with wired networks. MANET is a self-configuring network of mobile nodes connected by wireless links which form an arbitrary topology. The success of mobile ad hoc network (MANET) will depend on people's confidence in its security. This paper provides a survey of attacks and defensive technologies in MANETs. The countermeasures are features or functions that reduce or eliminate security vulnerabilities and attacks. The Ad hoc networks are a new wireless networking paradigm for mobile hosts. An Ad hoc network is selforganizing and adaptive. The network is ad hoc because it does not rely on a preexisting infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity.

III. CHAPTER 3 PROBLEM FORMULATION

3. TROJAN ATTACK IN AODV ROUTING PROTOCOL

Initially, we should take into account Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol and then we shall explain Trojan Attack.

3.1. Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol

Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol is used for finding a path to the destination in an ad-hoc network. To find the path to the destination all mobile nodes work in cooperation using the routing control messages. Thanks to these control messages, AODV Routing Protocol offers quick adaptation to dynamic network conditions, low processing and memory overhead, low network band width utilization with small size control messages. The most distinguishing feature of AODV compared to the other routing protocols is that it uses a destination sequence number for each route entry. The destination sequence number is generated by the destination when a connection is requested from it. Using the destination sequence number ensures loop freedom. AODV makes sure the route to the destination does not contain a loop and is the shortest path.

Route Requests (RREQs), Route Replay (RREPs), Route Errors (RERRs) are contro lmessages used for establishing a path to the destination, sent using UDP/IP protocols. Header information of these control messages are explained in [13]. When the source node wants to make a connection with the destination node, it broad cast an RREQ message. This RREQ message is propagated from the source, received by neighbors (intermediate nodes) of the source node. The intermediate nodes broadcast the RREQ message to their neighbors. This process goes on until the packet is received by destination node or an intermediate node that has a fresh enough route entry for the destination. Figure 9 shows how the RREQ message is propagated in an ad-hoc network.

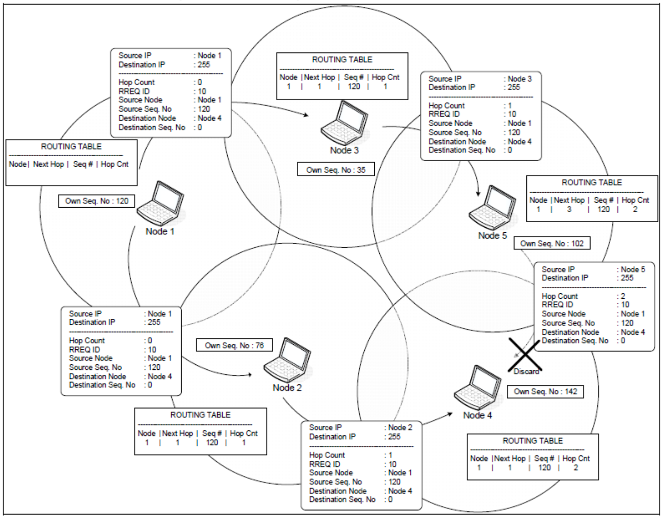


Figure 9 – Propagation of the RREQ message

Fresh enough means that the intermediate node has a valid route to destination formed a period of time ago, lower than the threshold. While the RREQ packet travels through the network, every intermediate node increases the hop count by one. If an RREQ message with the same RREQ ID is received, the node silently discards the newly received RREQs, controlling the ID field of the RREQ message. When the destination node or intermediate node that has fresh enough route to the destination receive the RREQ message they create an RREP message and update their routing tables with accumulated hop count and the sequence number of the destination node.

Afterwards the RREP message is unicasted to the source node. The difference between the broadcasting an RREQ and unicasting RREP can be seen from Figures 9 and 10. While the RREQ and the RREP messages are forwarded by intermediate nodes, intermediate nodes update their routing tables and save this route entry for 3 seconds, which is the ACTIVE_ROUTE_TIMEOUT constant value of AODV protocol. The default constant values of the AODV protocol are listed in appendix of RFC – 3561 [13]. Thus the node knows over which neighbor to reach at the destination. In terminology, the neighbor list for destination is labeled as "Precursor List". Figure 10shows how the RREP message is unicasted and how the route entries in the intermediate nodes are updated.

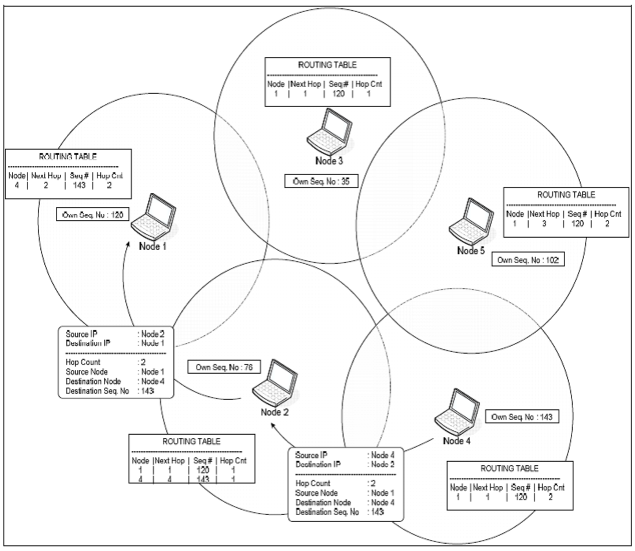


Figure 10 – Unicasting the RREP message

3.2. Sequence Numbers

Sequence Numbers serve as time stamps and allow nodes to compare how fresh their information on the other node is. However when a node sends any type of routing control message, RREQ, RREP, RERR etc., it increases its own sequence number. Higher sequence number is more accurate information and whichever node sends the highest sequence number, its information is considered and route is established over this node by the other nodes.

The sequence number is a 32-bit unsigned integer value (i.e., 4294967295). If the sequence number of the node reaches the possible highest sequence number, 4294967295, then it will be reset to zero (0). If the results of subtraction of the currently stored sequence number in a node and the sequence number of incoming AODV route control message is less than zero, the stored sequence number is changed with the sequence number of the incoming control message.

In Figure 11, while Node 2 forwards the RREP message coming from Node 3, it compares its own previously stored sequence number with that of Node 3. If it notices that the sequence number is newer than its own, then it changes its route table entry as necessary.

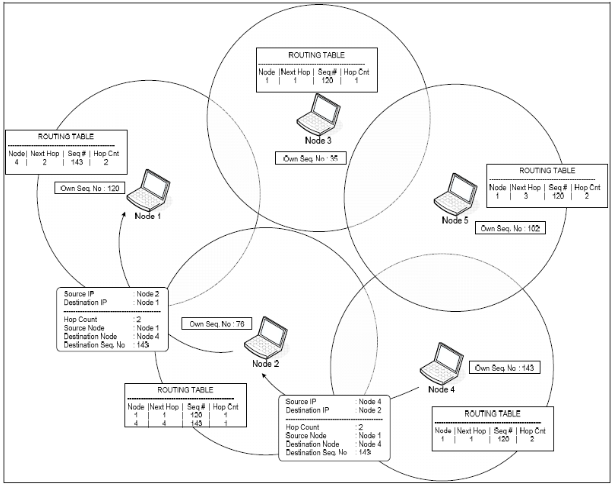


Figure 11 – Updating the Sequence Number with fresh one

3.3. Trojan Attack

Trojan Attack is briefly explained in the previous Chapter. In this Chapter we shall explain it in more detail as we have already explained the AODV protocol. In an ad-hoc network that uses the AODV protocol, a Trojan node absorbs the network traffic and drops all packets. To explain the Trojan Attack we added a malicious node that exhibits Trojan behavior in the scenario of the figures of the previous section.

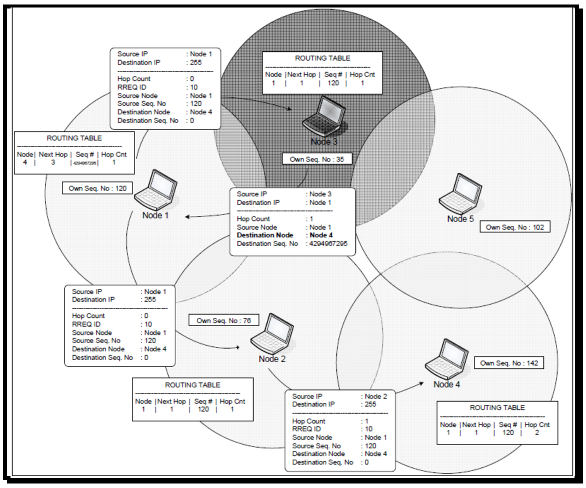


Figure 12 – Illustration of Trojan Attack

In this scenario shown in Figure 12, we assume that Node 3 is the malicious node. When Node 1 broadcasts the RREQ message for Node 4, Node 3 immediately responds to Node 1 with an RREP message that includes the highest sequence number of Node 4, as if it is coming from Node 4. Node 1 assumes that Node 4 is behind Node 3 with 1 hop and discards the newly received RREP packet come from Node 2. Afterwards Node 1 starts to send out its data packet to the node 3 trusting that these packets will reach Node 4 but Node 3 will drop all data packets.

In a Trojan Attack, after a while, the sending node understands that there is a link error because the receiving node does not send TCP ACK packets. If it sends out new TCP data packets and discovers a new route for the destination, the malicious node still manages to deceive the sending node. If the sending node sends out UDP data packets the problem is not detected because the UDP data connections do not wait for the ACK packets.

In our scenarios we use UDP data packets and we will explain our scenarios and their results in Chapter 5. Before Chapter 5 we will describe how Trojan behavior is implemented in the simulator program, MATLAB- 10.

IV. METHODOLOGY

4. Result, Discussion and Simulation

In this work, we have tried to evaluate the effects of the Trojan attacks in the wireless Ad-hoc Networks. To achieve this we have simulated the wireless ad-hoc network scenarios which includes Trojan node using MATLAB- 10[14] program. To simulate the Trojan node in a wireless ad-hoc network we have implemented a new protocol that drops data packets after attracting them to itself. In this chapter we present MATLAB- 10and our contribution to this software.

4.1. MATLAB- 10

MATLAB- 10 is an event driven MATLAB- 10 program, developed at the University of California Berkley, which includes many network objects such as protocols, applications and traffic source behavior. The MATLAB- 10 is a part of software of the VINT project [15] that is supported by DARPA since 1995.

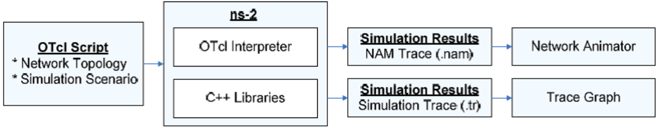


Figure 13 - MATLAB- 10 schema

At the simulation layer MATLAB- 10 uses OTcl (Object oriented Tool Command Language) programming language to interpret user simulation scripts. OTcl language is in fact an object oriented extension of the Tcl Language. The Tcl language is fully compatible with the C++ programming language. At the top layer, MATLAB- 10 is an interpreter of Tcl scripts of the users, they work together with C++ codes. In Chapter 5 the usage of the Tcl Language will be explained in detail.

As shown in Figure 13 [16], an OTcl script written by a user is interpreted by MATLAB- 10. While OTcl script is being interpreted, MATLAB- 10 creates two main analysis reports simultaneously. One of them is NAM (Network Animator) object that shows the visual animation of the simulation. The other is the trace object that consists of the ehavior of all objects in the simulation. Both of them are created as a file by MATLAB- 10. Former is .nam file used by NAM software that comes along with MATLAB- 10. Latter is a ".tr" file that includes all simulation traces in the text format.

MATLAB- 10 project is normally distributed along with various packages (MATLAB- 10, nam, tcl, otcl etc.) named as "all-in-one package", but they can also be found and downloaded separately. In this study we have used version 2.29 of MATLAB- 10 all-in-one package and installed the package in the Windows environment using Cygwin. After version 2, MATLAB- 10is commonly using a MATLAB- 10 and in our thesis we shell refer to it as MATLAB- 10. We have written the ".tcl" files in text editor and analyzed the results of the ".tr" file using"cat", "awk", and "wc" and "grep" commands of Unix Operating System. The implementation phase of the Trojan behavior to the AODV protocol is written using C++.

4.2 SIMULATION OF Trojan ATTACK AND ITS EFFECTS

In Chapter 3 we explained Trojan Attack in AODV Routing Protocol and in Chapter 4 we described how this attack is implemented into the MATLAB- 10. In this Chapter, first, we will briefly explain the Tcl Language to understand the simulation scenarios. Having shown how we tested the Trojan implementation, we will present the simulations of Trojan Attack to demonstrate its effects. Then we will evaluate the effects of Trojan Attack in an Ad-Hoc Networks.

4.4. Testing the Trojan AODV

We have tested our implementation of the Trojan to see whether it is correctly working or not. To be ensuring the implementation is correctly working, we used the NAM (Network Animator) application of MATLAB- 10. To test the implementation we used two simulations. In the first scenario we did not use any Trojan AODV Node(the malicious node that exhibits the Trojan Attack will be called "Trojan Node"). In the second scenario we added a Trojan AODV Node to the simulation. Then we compared the results of the simulations using NAM.

4.5 Simulation of Trojan Attack

4.5.1. Simulation Parameters and Measured Metrics

4.5.2. Evaluation of Results

Each scenario has two simulations. In the first one every node is working in cooperation with each other to keep the network in communication. The second simulation has one malicious node that carries out the Trojan Attack. In our study, we try to compare the results of these two simulations to understand the network and node behaviors.

We first try to evaluate the packet loss. Therefore we counted how many packets are sent by the sending nodes and how many of them reached the receiving nodes. In the previous section, we described how we obtain the numbers of the packets. The tables in the Appendix E compares the normal and Trojan networks. In the tables, the second column shows how many packets are sent by sending nodes and the third column shows how many of them reached the receiving nodes. By calculating the difference between the tables of normal and Trojan AODV network we try to evaluate how many of the packets which could not reach the destination node are absorbed in the Trojan Node. Packets lost in the Trojan Node are shown in the fourth column of the table of the Trojan network. The rest of the columns show percentage of the packets lost and additionally in the table of Trojan network, we added percentage of loss packets which are absorbed in the Trojan Node.

We noticed that the percentage of data loss of the Trojan AODV is increased more than the normal AODV network simulations in all scenarios. The first table of the Appendix G shows how the packet loss has increased. We also understand from tables the packet loss already exists in the network. This is because packets drop at the node interface queue due to the density of data traffic. To minimize the data traffic we alter node and packet parameters. Needing to evaluate the Trojan effect in the network, we have to minimize the packet loss which happens at the network, except the Trojan. In a wireless ad-hoc network which does not have any Trojan, the data traffic might be dense and packets might get lost, for instance in a FTP traffic. In our simulations of normal AODV network, we saw that data loss is increased up to 40% when we change parameters. Therefore, the data loss does not always say there was a Trojan Node in the network.

4.6 Solution for Trojan Attack and Its Effects

In the two previous chapters, we explain how Trojan Attack is implemented in MATLAB- 10 and which the results are obtained from the simulations. When we examine the trace file of the simulations that include one Trojan node, we saw that after a while second RREP message came to source node from the real destination node.

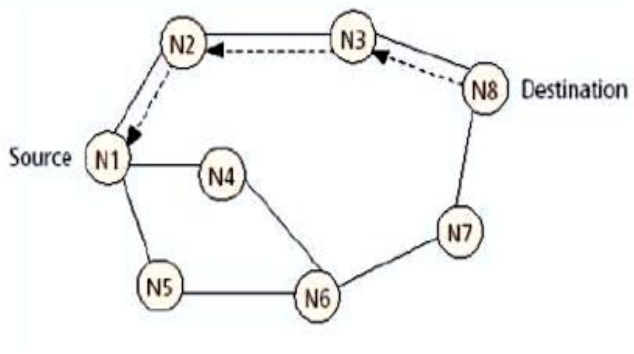


Figure 24 – Test simulation to show two RREP message

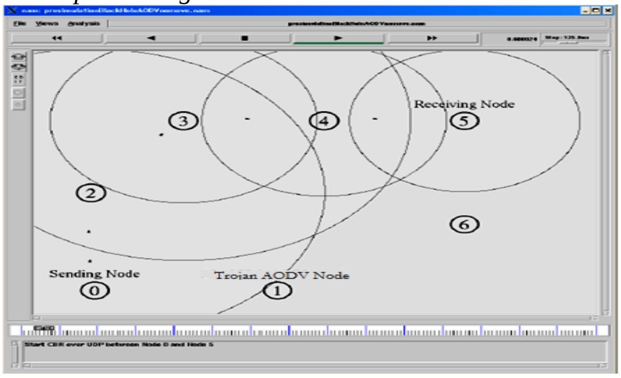
To figure out how the second packet came to source node, we created a simulation scenario with node positions shown in Figure 25. In the scenario, Node 0 is the sending node, Node 1 is Trojan node and Node 5 is the receiving node. In Table 3 we can easily see these two RREP messages. The first RREP message came from the Trojan node (Node 1) and reached the source node (Node 0) at “0.205976533” of simulation time. The second RREP message arrived from the destination node (Node 5) and reached the Sending Node at “1.276544989” of simulation time.

			MAC Header		IP Header		AOVD Packet			
Event	Time (-t)	Node ID (-Ni)	Destination Address (-Md)	Souce Address (-Ms)	Destination IP.Port Address (-Id)	Source IP.Port Address (-Is)	Packet Type (-Pc)	Destination Node (-Pd)	Destination Seq No (-Pds)	Hop Count (-Ph)
r	0.205976533	0	0	1	0.255	1.255	REPLY	5	-1	1
r	1.276544989	0	0	2	0.255	5.255	REPLY	5	4	4

Table 3 – Receiving two RREP messages

As the Trojan send an RREP message without checking the tables, we assume that it is more likely for the first RREP to arrive from the Trojan. In some cases, this idea may not work. For instance; the second RREP can be received at source node from an intermediate node which has fresh enough information about the destination node or the second RREP message may also came from the Trojan node if the real destination node is nearer than the Trojan node. These examples are extendable according to node condition in the network topology. In our work, we tried to find how this solution eliminates the Trojan effects in an AODV networkand if it deteriorates the network performance.

4.7.1. Implementing the Solution in MATLAB- 10



Start CBR over UDP between Node 0 and Node 5

Figure 27 - CBR packet are reached to destination node properly

In the test simulation, we ensured that the IDSAODV implementation is correctly working. Then, we performed the same simulations on the scenarios we used in this study to compare the performance of IDS approach.

4.9 Simulation of IDSAODV and Evaluation of Results

To be able to evaluate if our solution has succeeded we used same scenarios and simulation parameters as described at earlier chapter and also to be able to obtain the simulation results we used a similar batch file adapted for idsaodv. The tables in Appendix F compare IDSAODV network with Trojan network. Appendix G shows the solution affected the packet loss, but the concern we had at the beginning are valid.

V. RESULTS

5.1 Implementation process under MATLAB Considering AODV, DSR and DSDV

Modification: The nature of wireless network is that any node can join freely the network and can leave it. Nodes which want to attack join the network. The malicious node then later exploits the irregularities in the network amongst the nodes. It participates in the transmission process and later on some stage launches the message modification attack [16]. Impersonation: In wireless networks a node is free to move in and out of the network. There is no secure authentication process in order to make the network secure from malicious nodes. The attacker use MAC and IP spoofing in order to get identity of another node and hide into the network. This kind of attack is also known as spoofing attack [16]. Man in middle Attack: An attacker sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases, attacker may impersonate the sender to communicate with receiver or impersonate the receiver to reply to the sender. Selective Forwarding: In such attacks, malicious nodes may refuse to forward certain packets and simply drop them, ensuring that they are not propagated any further. An adversary will not, however, drop every packet. To avoid raising suspicions, the adversary instead selectively drops packets originating from a few selected nodes and forwards the remaining Traffic [19]. False Node: A false node involves the addition of a node by an adversary and causes the injection of malicious data. An intruder might add a node to the system that feeds false data or prevents the passage of true data. Insertion of malicious node is one of the most dangerous attacks that can occur. Malicious code injected in the network could spread to all nodes, potentially destroying the whole network, or even worse, taking over the network on behalf of an adversary.[18]

Passive Traffic Monitoring: It can be developed to identify the communication parties and functionality which could provide information to launch further attacks.

Eavesdropping: The term eavesdrops implies overhearing without expending any expending any extra effort. In this intercepting and reading and conversation of message by unintended receiver take place. Mobile host in mobile ad-hoc network shares a wireless medium. Majorities of wireless communication use RF spectrum and broadcast by nature.

Message transmitted can be eavesdropped and fake message can be injected into network.

Traffic Analysis: Traffic analysis is a passive attack used to gain information on which nodes communicate with each other and how much data is processed.

Syn flooding: This attack is denial of service attack. An attacker may repeatedly make new connection request until the resources required by each connection are exhausted or reach a maximum limit. It produces severe resource constraints for legitimate nodes.

CONCLUSION: The deployment of sensor nodes in an unattended environment makes the networks vulnerable. Wireless sensor networks are increasingly being used in military, environmental, health and commercial applications. In this thesis, we have analyzed security attacks its prerequisite and vulnerability for processing and collecting the information in WSN and presented the security objective that need to be achieved.

5.2. Integrated Proposed Model

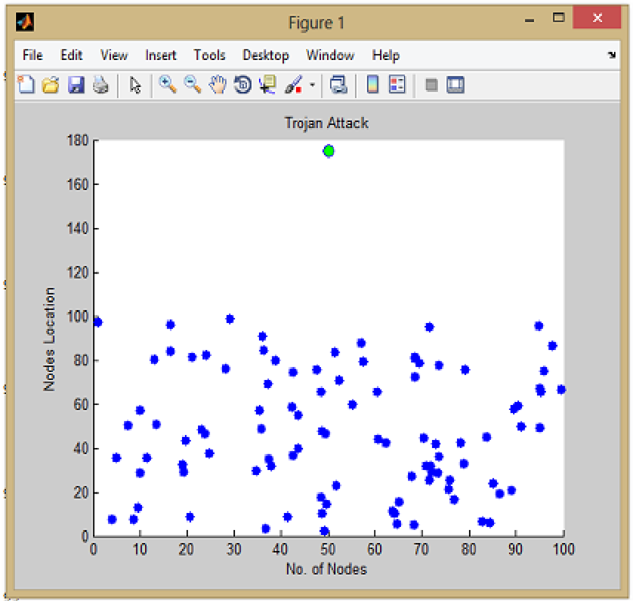
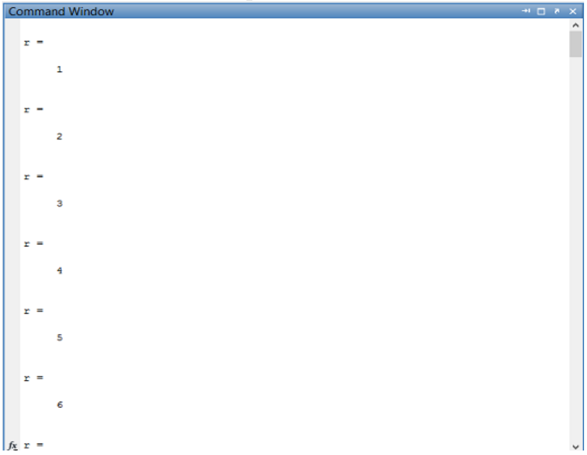


Figure 28–No. of nodes 100 for Trojan Attack Using AODV protocol



```
r =

     1

r =

     2

r =

     3

r =

     4

r =

     5

r =

     6

fx r =
```

Figure 29–No. of Rounds from 1 to 6 which is shown here for Trojan Attack Using AODV Protocol

```
r =

    94

r =

    95

r =

    96

r =

    97

r =

    98

r =

    99

fx >> |
```

Figure 30 - No. of Rounds from 94 to 99 which is shown here for Trojan Attack Using AODV (Total No. of Rounds 99)

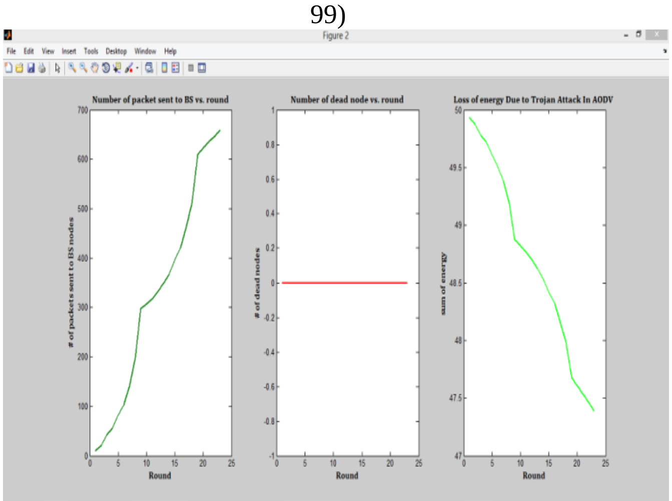


Figure 31: (1)-Number of Packets Sends To BS Vs Rounds (2) Number of Dead Nodes vs. Round (3) Loss of Energy Due to Trojan Attack in AODV in Different Rounds

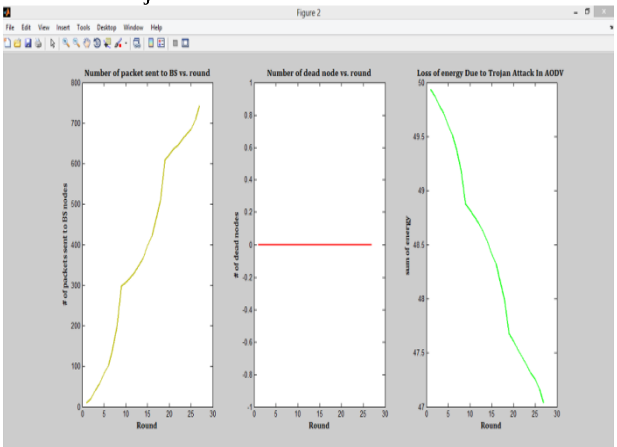


Figure 32: (1)-Number of Packets Sends To BS Vs Rounds (2) Number of Dead Nodes vs. Round (3) Loss of Energy Due to Trojan Attack Attack in AODV in Different Rounds

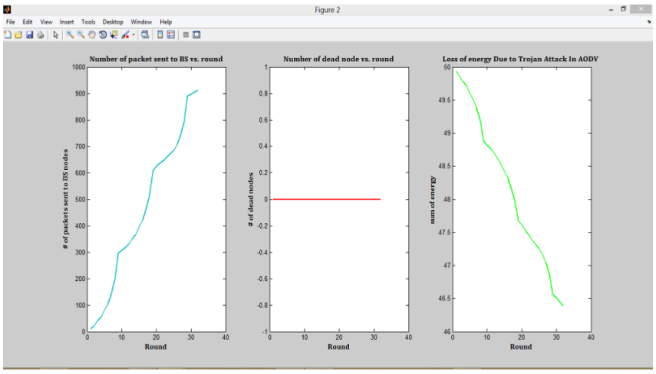


Figure 2
File Edit View Insert Tools Desktop Window Help
Number of packet sent to BS vs. round
# of packets sent to BS nodes
0
100
200
300
400
500
600
700
800
900
1000
0
10
20
30
40
Round
Number of dead node vs. round
# of dead nodes
-1
-0.8
-0.6
-0.4
-0.2
0
0.2
0.4
0.6
0.8
1
Round
Loss of energy Due to Trojan Attack In AODV
sum of energy
46
46.5
47
47.5
48
48.5
49
49.5
50
Round

Figure 33: (1)-Number of Packets Sends To BS Vs Rounds (2) Number of Dead Nodes vs. Round (3) Loss of Energy Due to Trojan Attack in AODV in Different Rounds

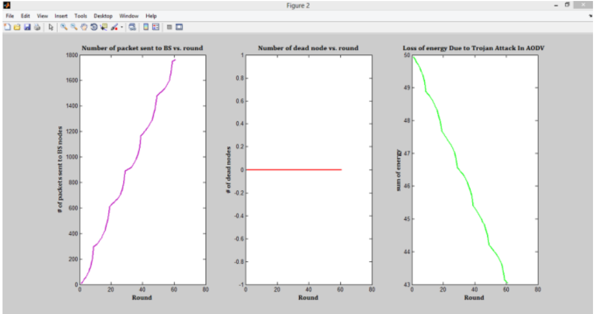


Figure 2
File Edit View Insert Tools Desktop Window Help
Number of packet sent to BS vs. round
# of packets sent to BS nodes
0
200
400
600
800
1000
1200
1400
1600
1800
0
20
40
60
80
Round
Number of dead node vs. round
# of dead nodes
-1
-0.8
-0.6
-0.4
-0.2
0
0.2
0.4
0.6
0.8
1
Round
Loss of energy Due to Trojan Attack In AODV
sum of energy
43
44
45
46
47
48
49
50
Round

Figure 34: (1)-Number of Packets Sends To BS Vs Rounds (2) Number of Dead Nodes vs. Round (3) Loss of Energy Due to Trojan Attack in AODV in Different Rounds

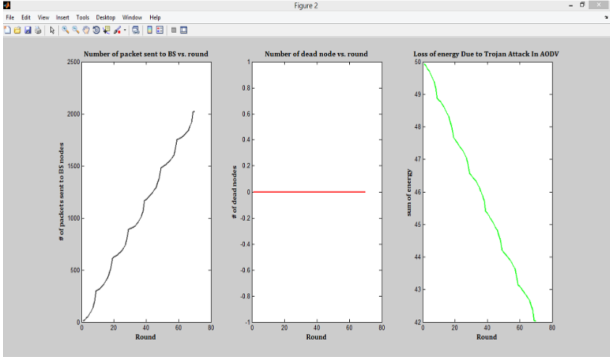


Figure 2
File Edit View Insert Tools Desktop Window Help
Number of packet sent to BS vs. round
# of packets sent to BS nodes
0
500
1000
1500
2000
2500
0
20
40
60
80
Round
Number of dead node vs. round
# of dead nodes
-1
-0.8
-0.6
-0.4
-0.2
0
0.2
0.4
0.6
0.8
1
Round
Loss of energy Due to Trojan Attack In AODV
sum of energy
42
43
44
45
46
47
48
49
50
Round

Figure 35: (1)-Number of Packets Sends To BS Vs Rounds (2) Number of Dead Nodes vs. Round (3) Loss of Energy Due to Trojan Attack inAODV in Different Rounds

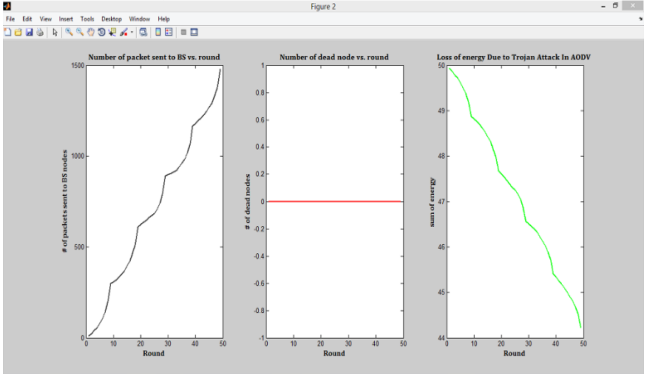


Figure 2
File Edit View Insert Tools Desktop Window Help
Number of packet sent to BS vs. round
# of packets sent to BS nodes
0
500
1000
1500
0
10
20
30
40
50
Round
Number of dead node vs. round
# of dead nodes
-1
-0.8
-0.6
-0.4
-0.2
0
0.2
0.4
0.6
0.8
1
Round
Loss of energy Due to Trojan Attack In AODV
sum of energy
44
45
46
47
48
49
50
Round

Figure 36: (1)-Number of Packets Sends To BS Vs Rounds (2) Number of Dead Nodes vs. Round (3) Loss of Energy Due to Trojan Attack in AODVafter99 Rounds

VI. CONCLUSION AND FUTURE WORK

6.1 Conclusion

In this study, we analyzed effect of the Trojan in an AODV Network. For this purpose, we implemented an AODV protocol that behaves as Trojan in MATLAB- 10. We simulated five scenarios where each one has 20 nodes that use AODV protocol and also simulated the same scenarios after introducing one Trojan Node into the network. Moreover, we also implemented a solution that attempted to reduce theTrojan effects in MATLAB- 10 and simulated the solution using the same scenarios. Our simulation results are analyzed below:

Having simulated the Trojan Attack, we saw that the packet loss is increased in the ad-hoc network. In Appendix E, tables of simulation results show the difference between the number of packets lost in the network with and without a Trojan Attack. This also shows that Trojan Attack affects the overall network connectivity and the data loss could show the existence of the Trojan Attack in the network. If the number of Trojan Nodes is increased then the data loss would also be expected to increase.

We can understand from Appendix G; AODV network has normally 3 to 21 % data loss and if a Trojan Node is introducing in this network data loss is increased to 92 to 59 %. As 3 to 21 % data loss already exists in this data traffic, Trojan Node increases this data loss by 89 to 38 %. When we used IDSAODV protocol in the same network, the data loss decreased to 65 %. These two results show that our solution reduces the Trojan effects by 24-38 % as packet loss in a network using IDSAODV and where there is no Trojans increases to 75-62 %.

6.2. Future Work

We simulated the Trojan Attack in the Ad-hoc Networks and investigated its affects. In our study, we used the AODV routing protocol. But the other routing protocols could be simulated as well. All routing protocols are expected to present different results. Therefore, the best routing protocol for minimizing the Trojan Attack may be determined. In our thesis, we try to eliminate the Trojan effect in the network. But detection of the Trojan Node is another future work. In our work, we assume the Trojan node is detected and tried to eliminate its effects. There are many Intrusion Detection Systems (IDS) for ad-hoc networks. These IDSs could be tested to determine which one is the best to detect the Trojan. Our solution tries to eliminate the Trojan effect at the route determination mechanism of the AODV protocol that is carried out before the nodes start the packets. Additionally, we used UDP connection to be able to count the packets at sending and receiving nodes. If we had used the TCP connection between nodes, the sending node would be the end of the connection, since ACK packets do not reach the sending node. This would be another solution for finding the Trojan Node. This takes place after the route determination mechanism of the ADOV protocol and finds the route in a much longer period. Our solution finds the path in the AODV level. Finding the Trojan node with connection oriented protocols could be another work as a future study.

REFERENCE

[1] Sanjeet1, Asst Prof. Sonia Rani2 "Detection And Elimination Of Trojan Attack In Manet" International Journal For Technological Research In Engineering Volume 2, Issue 12, August-2015 ISSN (Online): 2347 – 4718. www.ijtre.com Copyright 2015.All rights reserved. 2996.

[2] Sureka.N1, Prof. S. Chandra Sekaran "Securable Routing And Elimination Of Adversary Attack From Manet" ISSN(Online): 2320-9801 ISSN (Print): 2320-9798 International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014 Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14) Organized by Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014 Copyright @ IJIRCCE www.ijircce.com 4068.

[3] Harsha.N1, Rashmi.S "Detection of Vampire Attack and Prevention in MANET" ISSN (Online) 2278-1021 ISSN (Print) 2319 5940 International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 8, August 2015. Copyright to IJARCCE DOI 10.17148/IJARCCE.2015.4872 340.

[4] Sumit Agrawal, Shilpa Jaiswal "Study to Eliminate Threat of Black Hole of Network Worms in MANET" International Journal of Scientific and Research Publications, Volume 2, Issue 9, September 2012 1 ISSN 2250-3153 www.ijsrp.org.

[5] Saritha Reddy Venna1, Ramesh Babu Inampudi "Security Attacks in Mobile Ad Hoc Networks" Saritha Reddy Venna et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (1), 2016, 135-140.

[6] Guozhu Meng, Yang Liu, Jie Zhang, Alexander Pokluda, Raouf Boutaba "Collaborative Security: A Survey and Taxonomy" USA, fax +1 (212) 869-0481, or ACM 0360-0300/YYYY/01-ARTA $15.00 DOI:http://dx.doi.org/10.1145/0000000.0000000 ACM Computing Surveys, Vol. V, No. N, Article A, Publication date: January YYYY.

[7] K.Sivakumar1, P.Murugapriya "Efficient Detection and Elimination of Vampire Attacks in Wireless Ad-Hoc Sensor Networks" ISSN(Online): 2320-9801 ISSN (Print): 2320-9798 International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014 Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14) Organized by Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014. Copyright @ IJIRCCE www.ijircce.com 596.

[8] Manju.V.C. "Wireless Sensor Network Attacks" ISSN: 2277-3754 ISO 9001:2008 Certified International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 2, August 2012.

[9] Ambili M A1, BijuBalakrishnan "A Security Approach For Detection And Elimination Of Resource Depletion Attack In Wireless Sensor Network" ISSN(Online): 2320-9801 ISSN (Print): 2320-9798 International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014 Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14) Organized by Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014.

[10] Varalatchoumy.M, Sowmya H.K. Kohilambal R "Security Attacks and Defensive Technologies in MANETs" Proc. of the Intl. Conf. on Computer Applications – Volume 1. Copyright © 2012 Techno Forum Group, India. ISBN: XXXXXXX :: doi: 10.XXXXX/ISBN_0768 ACM #: dber.imera.10.XXXXX

[11] Y.-C. Hu, D. B. Johnson, and A. Perrig, "Sead: Secure efficient distance vector routing for mobile wireless ad-hoc networks," in WMCSA '02: Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications. Washington, DC, USA: IEEE Computer Society, 2002, 3–13.

[12] X. Wang, T. liang Lin, and J. Wong, Feature Selection in Intrusion Detection System over Mobile Ad-hoc Network. Technical Report,Computer Science, Iowa State University, 2005.

[13] J. Grønkvist, A. Hansson, and M. Skøld, Evaluation of a Specification-Based Intrusion Detection System for AODV.di.ionio.gr/medhocnet07/wp content/uploads/papers/90.pdf, 2007.

[14] S. Kurosawa, H. Nakayama, and N. Kato, "DetectingTrojanattackon AODV based mobile ad-hoc networks by dynamic learning method, "International Journal of Network Security, pp. 338–346, 2007.

[15] K. Makki, N. Pissinou, and H. Huang, "Solutions to the Trojanproblem in mobile ad-hoc network," 5th World Wireless Congress, pp.508–512, 2004.

[16] S. Lu, L. Li, K.Y. Lam, L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Trojan Attack.," International Conference on Computational Intelligence and Security, 2009.

[17] Chang Wu Yu, Wu T-K, Cheng RH, Shun chao chang, "A Distributed and Cooperative Trojan Node Detection. And Elimination Mechanism for Ad Hoc Network", Emerging Technologies in knowledge Discovery and Data Mining, Vol. 4819, Issue 3, pp 538-549,2007.