IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

Efficient Policy based Detection of Jamming Attacks in MANETS

R.Akila[1], Mabel P Jenefer[2]

Assistant Professor, Department of Computer Technology, Sri Krishna Arts and Science College,

Coimbatore, Tamil Nadu, India[1]

Student, Department of Computer Technology, Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India[2]

Abstract: A mobile Ad Hoc network (MANET) may be a wireless network that doesn't consider any fastened infrastructure (i.e., routing facilities, such as wired networks and access points), and whose nodes should coordinate among themselves to see property and routing. the standard way of protective networks isn't directly applicable to MANETs. Many conventional security solutions are ineffective and inefficient for the highly dynamic and resource-constrained environments wherever Edouard Manet use may be expected. Since bar techniques are ne'er enough, intrusion detection systems (IDSs), that monitor system activities and detect intrusions, are typically accustomed complement alternative security mechanisms. the way to discover intrusions effectively and expeditiously on this highly dynamic, distributed and resource-constrained setting may be a challenging analysis drawback. during this paper, we tend to investigate the employment of evolutionary computation techniques for synthesizing intrusion detection programs on MANETs. we tend to evolve programs to discover the subsequent attacks against MANETs: dropping attacks and power consumption attack. The planned system may be a novel design that uses knowledge-based intrusion discovering techniques to detect the attacks that an antagonist will perform against the routing cloth of mobile impromptu networks. Mobile unexpected Networks (MANETs) are vulnerable to various node misbehaviours attributable to their distinctive options, such as highly dynamic topology, rigorous power constraints and error-prone transmission media. important analysis efforts have been created to deal with the matter of misbehaviour detection. However, very little analysis work has been done to differentiate reallymalicious behaviours from the faulty behaviours. each the malicious behaviours and therefore the faulty behaviours are typically equally treated as misbehaviours with none additional investigation by most of the traditional misbehaviour detection mechanisms. during this paper, we propose and develop a policy-based malicious peer detection mechanism, within which context data, like communication channel standing, buffer standing, and transmission power level, is collected so wont to confirm whether or not the misbehaviour is likely a results of malicious activity or not. Simulation results illustrate that the policy-based malicious peer detection mechanism is able to differentiate malicious peers from faulty peers with high confidence. Moreover, the mechanism converges to an even view of malicious nodes amongst all the nodes with a restricted communication overhead.

Index Terms: MANET, Jamming, Attack, Intrusion Detection, Network Gateway, Infrastructure.

I. INTRODUCTION

MOBILE Ad hoc Networks (MANET) are utilized to set up wireless communication in improvised environments without a predefined infrastructure or centralized administration. Therefore, MANET has been normally deployed in adverse and hostile environments where central authority point is not necessary. Another unique characteristic of MANET is the dynamic nature of its network topology which would be frequently changed due to the unpredictable mobility of nodes.

Furthermore, each mobile node in MANET plays a router role while transmitting data over the network. Hence, any compromised nodes under an adversary's control could cause significant damage to the functionality and security of its network since the impact would propagate in performing routing tasks. Several work addressed the intrusion response actions in MANET by isolating uncooperative nodes based on the node reputation derived from their behaviors. Such a simple response against malicious nodes often neglects possible negative side effects involved with the response actions. In MANET scenario, improper countermeasures may cause the unexpected network partition, bringing additional damages to the network infrastructure. To address the above-mentioned critical issues, more flexible and adaptive response should be investigated. The notion of risk can be adopted to support more adaptive responses to routing attacks in MANET.

The original definition of OLSR does not include any provisions for sensing of link quality; it simply assumes that a link is up if a number of packets have been received recently. This assumes that links are bi-modal (either working or failed), which is not necessarily the case on wireless networks, where links often exhibit intermediate rates of packet loss.

To encrypt the data which has been sent from sender to receiver a technique named Rijndael encryption method.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

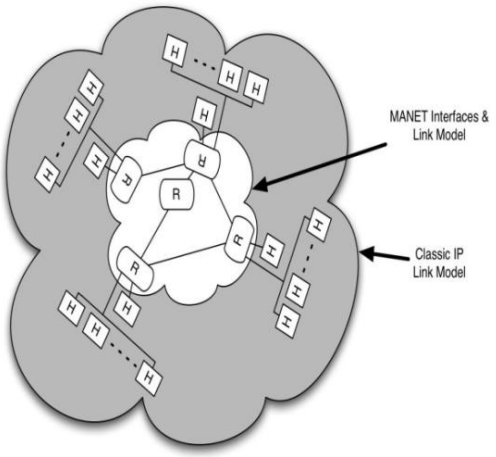


Fig.1.1 MANET Architecture

Due to natural mobility and scalability, wireless networks are always preferred since the first day of their invention. Owing to the improved technology and reduced costs, wireless networks have gained much more preferences over wired networks in the past few decades. By definition, Mobile Ad hoc NETwork (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. Industrial remote access and control via wireless networks are becoming more and more popular these days . One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. However, this communication is limited to the range of transmitters. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own.

MANET solves this problem by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multihop. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multihop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. In contrary to the traditional wireless network, MANET has a decentralized network infrastructure. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly . MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances where an infrastructure is unavailable or unfeasible to install in scenarios like natural or human-induced disasters, military conflicts, and medical emergency situations

Many current and envisaged applications for Wireless Sensor Networks (WSNs) involve data collection in remote, inaccessible or hostile environments, such as deserts, mountains, ocean floors and battlefields. A multitude of sensors might be deployed within a certain area and their activity is usually monitored and managed by a powerful trusted entity, commonly referred to as the sink. Security in WSNs presents several well-known challenges stemming from all kinds of resource constraints of individual sensors. However, resource limitations is not the main challenge in designing security techniques for WSNs. It is lack of ubiquitous (inexpensive) tamper-resistant hardware that makes sensor compromise a real threat. Some recent results showed that commodity sensors can be easily corrupted. Once a sensor is corrupted and all of its secrets are exposed, any cryptographic protocol ceases to be effective.

Based on the time of corruption, we can view the security state of a given sensor as a sequence of three epochs: (1) time before corruption; (2) time during corruption; and (3) time following corruption. Nothing can be done about security in epoch 2 as the adversary controls the sensor, while enforcing security in epochs 1 and 3 requires forward and backward secrecy, respectively. Informally, a cryptographic protocol is forward secureif exposure of secret material at a given time does not lead to compromise of secrets for any time preceding compromise. Whereas, a cryptographic protocol is backward secure if compromise of secret material at a given time does not lead to compromise of any secrets to be used in future. It is well-known that forward secrecy can be easily obtained by periodically evolving a secret (e.g., a key), using a one-way function. If we assume that time is divided in rounds and let K0 be an initial secret, the secret for round $r \geq 1$ (Kr) is computed as H(Kr−1), where H(•) is a one-way function. Hence, if the adversary learns secret Kr, it cannot compute any secrets used in prior rounds. However, backward security is much more challenging, since knowledge of Kr allows the adversary to compute secrets for future rounds by mimicking the secret evolution procedure.

Note that this is possible even if the adversary is no longer in control of a given sensor in round r_. Backward secrecy would be trivial to obtain if each sensor had a true random number generator (TRNG). Because a TRNG yields information-theoretically independent values, even if the adversary learns many (but not all) TRNG outputs, it cannot compute the missing values, whether they correspond to the past or to the future. Unfortunately, TRNGs are not found on commodity sensors and not expected to be available for the near future. An alternative to per-sensor TRNGs is the presence of a trusted third party; this is assumed in key-insulated schemes . In such schemes, forward and backward security is achieved by having end-devices evolve their secrets in cooperation with a trusted third party, called a base. Unless both the end-device and the base are compromised at the same time, per-round keys are insulated. Key-insulated schemes are well-matched for WSNs with a constantly present sink, where the latter acts as a base. However, in Unattended

DOI 10.17148/IJARCCE.2016.5378

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

WSNs (UWSNs), the sink visits the network infrequently, which rules out key-insulated schemes.

A **mobile ad hoc network** (**MANET**) is a self-configuring infrastructurelessnetwork of mobile devices connected by wireless. Ad hoc is Latin and means "for this purpose".Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router.

The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet.MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network.

The growth of laptops and 802.11/Wi-Fi wireless networking have made MANETs a popular research topic since the mid-1990s. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measures such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc.

Data Monitoring and Mining Using MANETs

MANETS can be used for facilitating the collection of sensor data for data mining for a variety of applications such as air pollution monitoring and different types of architectures can be used for such applications. It should be noted that a key characteristic of such applications is that nearby sensor nodes monitoring an environmental feature typically register similar values. This kind of data redundancy due to the spatial correlation between sensor observations inspires the techniques for in-network data aggregation and mining. By measuring the spatial correlation between data sampled by different sensors, a wide class of specialized algorithms can be developed to develop more efficient spatial data mining algorithms as well as more efficient routing strategies. Also researchers have developed performance models for MANET by applying Queueing Theory.

Security of MANETs

A lot of research was done in the past but the most significant contributions were the PGP (Pretty Good Privacy) and the trust based security but none of the protocols made a decent tradeoff between security and performance. In an attempt to enhance security in MANETs many researchers have suggested and implemented new improvements to the protocols and some of them have suggested new protocols.

Classification of Attacks on MANETs

These attacks on MANETs challenge the mobile infrastructure in which nodes can join and leave easily with dynamics requests without a static path of routing. Schematics of various attacks as described by Al-Shakib Khan on individual layer are as under:

- Application Layer: Malicious code, Repudiation
- Transport Layer: Session hijacking, Flooding
- Network Layer: Sybil, Flooding, Black Hole, Grey Hole. Worm Hole, Link Spoofing, Link Withholding, Location disclosure etc.
- Data Link/MAC: Malicious Behaviour, Selfish Behaviour, Active, Passive, Internal External
- Physical: Interference, Traffic Jamming, Eavesdropping

An **intrusion detection system** (**IDS**) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization. IDPSes typically record information related to observed events, notify security administrators of important observed events and produce reports. Many IDPSes can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g. reconfiguring a firewall) or changing the attack's content
One preliminary IDS concept consisted of a set of tools intended to help administrators review audit trails. User access logs, file access logs, and system event logs are examples of audit trails.

II. BACKGROUND STUDY

Anonymity, unobservability, and pseudonymity: a consolidated proposal for terminology

Based on the nomenclature of the early papers in the field, we propose a terminology which is both expressive and precise. More particularly, we define anonymity, unsinkability, unobservability, pseudonymity (pseudonyms and digital pseudonyms, and their attributes), and identity management. In addition, we describe the relationships between these terms, give a rational why we define them as we do, and sketch the main mechanisms to provide for the properties defined.

In order to quantify anonymity within concrete situations, one would have to describe the system in sufficient detail which is practically not (always) possible for large open systems (but maybe for some small data bases for instance). Besides the quantity of anonymity provided within a particular setting, there is another aspect of anonymity: its robustness. Robustness of anonymity characterizes how stable the quantity of anonymity is

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

against changes in the particular setting, e.g. a stronger attacker or different probability distributions. We might use quality of anonymity as a term comprising both quantity and robustness of anonymity. To keep this text as simple as possible, we will mainly discuss the quantity of anonymity in the sequel, using the wording "strength of anonymity".

One might differentiate between the term anonymity and the term in distinguish ability, which is the state of being indistinguishable from other elements of a set. In distinguish ability is stronger than anonymity as defined in this text. Even against outside attackers, in distinguish ability does not seem to be achievable without dummy traffic. Against recipients of messages, it does not seem to be achievable at all.

On Flow Correlation Attacks and Countermeasures in Mix Networks

issues related to flow correlation attacks and the corresponding countermeasures in mix networks. Mixes have been used in many anonymous communication systems and are supposed to provide countermeasures that can defeat various traffic analysis attacks. In this paper, we focus on a particular class of traffic analysis attack, flow correlation attacks, by which an adversary attempts to analyse the network traffic and correlate the traffic of a flow over an input link at a mix with that over an output link of the same mix. Two classes of correlation methods are considered, namely time-domain methods and frequency-domain methods. Based on our threat model and known strategies in existing mix networks, we perform extensive experiments to analyse the performance of mixes. We find that a mix with any known batching strategy may fail against flow correlation attacks in the sense that for a given flow over an input link, the adversary can correctly determine which output link is used by the same flow. We also investigated methods that can effectively counter the flow correlation attack and other timing attacks. The empirical results provided in this paper give an indication to designers of Mix networks about appropriate configurations and alternative mechanisms to be used to counter flow correlation attacks.

We formally model the behaviour of an adversary who launches flow correlation attacks. In order to successfully identify the output port of an incoming flow, the flow correlation attack must accurately measure the similarity of traffic flows into and out of a mix. Two classes of correlation methods are considered, namely time-domain methods and frequency-domain methods. In the time domain, mutual information is used to measure the traffic similarity. In the frequency domain, a matched filter based on the Fourier spectrum and the Wavelet spectrum is utilized. _We measure the effectiveness of a number of popular mix strategies in countering flow correlation attacks. Mixes with any tested batching strategy may fail under flow-correlation attacks in the sense that, for a given flow over an input link, the adversary can effectively detect which output link is used by the same flow.

We use Detection rate as the measure of success for the attack, where Detection rate is defined as the probability that the adversary correctly correlates flows into and out of a mix. We will show that, given a sufficient amount of data, known mix strategies fail, that is, the attack achieves close to 100% detection rate. This remains true, even in batching strategies that sacrifice QoS concerns (such as a significant TCP good put reduction) in favour of security. _While many mix strategies rely on other mechanisms in addition to batching alone, it is important to understandthe vulnerability of batching. In our experiments, we illustrates the dependency between attackeffectiveness for various batching strategies and the amount of data at hand for the attacks. These resultsshould guide mix designers in the educated choice of strategy parameters, such as for striping or for pathrerouting.

Untraceable electronic mail, return addresses, and digital pseudonyms

A technique based on public key cryptography is presented that allows an electronic mail system to hide who a participant communicates with as well as the content of the communication - in spite of an unsecured underlying telecommunication system. The technique does not require a universally trusted authority. One correspondent can remain anonymous to a second, while allowing the second to respond via an untraceablereturn address.

The technique can also be used to form rosters of untraceable digital pseudonyms from selected applications. Applicants retain the exclusive ability to form digital signatures corresponding to their pseudonyms. Elections in which any interested party can verify that the ballots have been properly counted are possible if anonymously mailed ballots are signed with pseudonyms from a roster of registered voters. Another use allows an individual to correspond with a record-keeping organization under a unique pseudonym which appears in a roster of acceptable clients.

Cryptology is the science of secret communication. Cryptographic techniques have been providing secrecy of message content for thousands of years . Recently some new solutions to the "key distribution problem" (the problem of providing each communicant with a secret key) have been suggested, under the name of public keycryptography.

Another cryptographic problem, "the traffic analysis problem" (the problem of keeping confidential who converses with whom, and when they converse), will become increasingly important with thegrowth of electronic mail. This paper presents a solution to the traffic analysis problem that is based on public key cryptography. Baran has solved the traffic analysis problem for networks , but requires each participant to trust a common authority. In contrast, systems based on the solution advanced here can be compromised only by subversion or conspiracy of all of a set of authorities. Ideally, each participant is an authority.

DOI 10.17148/IJARCCE.2016.5378

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

Self-Organized Public-Key Management for Mobile Ad Hoc Networks

In contrast with conventional networks, mobile ad hoc networks usually do not provide on-line access to trustedauthorities or to centralized servers and they exhibit frequent partitioning due to link and node failures and to node mobility. For these reasons, traditional security solutions that require on-line trusted authorities or certificaterepositories are not well suited for securing ad hoc networks. In this paper, we propose a fully self-organizedpublic-key management system that allows users to generate their public-private key pairs, to issue certificates, andto perform authentication regardless of the network partitions and without any centralized services. Furthermore,our approach does not require any trusted authority, not even in the system initialization phase

The main problem of any public-key based security system is to make each user's public key available to others in such a way that its authenticity is verifiable. In mobile ad hoc networks, this problem becomes even more difficult to solve because of the absence of centralized services and possible network partitions. More precisely, two users willing to authenticate each other are likely to have access only to a subset of nodes of the network (possibly those in their geographic neighborhood). The best known approach to the public-key management problem is based on public-key certificates . A public-key certificate is a data structure in which a public key is bound to an identity (and possibly to some other attributes) by the digital signature of the issuer of the certificate. In our system, like in PGP , users' public and private keys are created by the users themselves. For simplicity, we assume that each honest user owns a single mobile node. Hence, we will use the same identifier for the user and her node (i.e., both user u and her node will be denoted by u). Unlike in PGP, where certificates are mainly stored in centralized certificate repositories, certificates in our system are stored and distributed by the nodes in a fully self-organized manner. Each certificate is issued with a limited validity period and therefore contains its issuing and expiration times. Before a certificate expires, its issuer issues an updated version of the same certificate, which contains an extended expiration time.

ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Adhoc Networks

In hostile environments, the enemy can launch traffic analysis against interceptable routing information embedded in routing messages and data packets. Allowing adversaries to trace network routes and infer the motion pattern of nodes at the end of those routes may pose a serious threat to covert operations. We propose ANODR, an anonymous on-demand routing protocol for mobile ad hoc networks deployed in hostile environments. We address two closelyrelated problems: For route anonymity, ANODR prevents strong adversaries from tracing a packet flow back to its source or destination; for location privacy, ANODR ensures that adversaries cannot discover the real identities of local transmitters. The design of ANODR is based on "broadcast with trapdoor information", a novel network security concept which includes features of two existing network and security mechanisms, namely "broadcast" and "trapdoor information

Suppose a covert mission is launched, which includes swarms of reconnaissance, surveillance, and attack task forces. The ad hocnetwork must provide routes between command post and swarms (for delivery of reliable commands/controls from commander to swarms and for situation data/video reporting from swarms to the commander) as well as routes between swarms (data fusion, failure recovery, threat evasion etc). Providing anonymity and location privacy supports for the task forces is critical, else the entire mission may be compromised. This poses challenging constraints on routing and data forwarding. In fact, the adversary could deploy reconnaissance and surveillance forces in the battlefield and maintains communications among them. They could form their own network to infer the location, movement, number of participants, and even the goals of our covert missions.

On-demand routing schemes are more "covert" in nature in that they do not advertise in advance—they just set up routes as needed. Nevertheless, the enemy may gain a lot of information about the mission by analyzing on-demand routing information and observing packet flows once the connection is established. Since a necessary byproduct of any mission, whether covert or not, is communications across swarms and to/from command post, these flows and the routes temporarily set up at intermediate nodes must be protected from inference and intrusion.

Existing Research

Implementation of a policyenforcing mechanism based on a kernel-level trusted executionmonitor. Under this mechanism, each MANET application orprotocol has its own policy 1. All nodes supporting a certainapplication and enforcing its policy form a trusted applicationcentricnetwork. Since an application may depend on otherapplications, our policy enforcing mechanism creates a trusted multi-tier network. The member nodes in such a network mustenforce the policies associated with these applications as well.For instance, a peer-to-peer file sharing application may dependon an on-demand routing protocol. In this case, the mechanismcreates a two-tier trusted file sharing network. It first establishesa trusted routing tier, and hence a trusted network for routing,comprising of all the nodes that enforce the routing policy. Ontop of this tier, it then creates a file sharing tier, enforcing the filesharing policy.

In our policy enforcing mechanism, nodes can be members ofmultiple multi-tier networks simultaneously. For example, let usconsider that a vehicular traffic monitoring application uses thesame routing algorithm with the file sharing application. Nodesin the aforementioned file sharing network can also establish atraffic monitoring network by creating, on top of the routing tier,a separate

DOI 10.17148/IJARCCE.2016.5378

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

trusted tier enforcing the traffic monitoring policy. Twonodes may communicate through an application if and only if theyenforce the same application tier policy and all the underlying tierpolicies.Our policy enforcing mechanism allows each node to uniformlyenforce the policies without assuming any prior trust with othernodes. This is similar to the method of building trusted adhoc network we developed previously.

To ensure trusted policy enforcement, we augment each node with a trusted agent,which protects the policy enforcement components from beingcompromised. When a node joins a trusted tier, its trustedagent helps establish trust by proving the execution of a correcttrusted agent, a trustworthy policy enforcing software component(referred to as policy enforcerhereafter), and the right policy.Furthermore, it ensures that the integrity of the agent, the enforcer,and the policy will not be compromised. This is possible becausethe trusted agent is part of the operating system kernel andguarantees the integrity of the kernel and all programs involved inpolicy enforcement. Therefore, it can foil attacks, including thoselaunched by local users, to tamper with the enforcer or the policybeing enforced. If any of these components is compromised, thetrusted agent will disconnect the node from the trusted network.The trusted agent is built on top of Satem , our trusted execution monitor based on a low-end trusted hardware, TrustedPlatform Module (TPM) specified by the Trusted ComputingGroup (TCG)). Due to its low cost and broad support bycomputer makers, the TCG TPM has been already integrated inmany laptops. In the near future, it will also be installed on smallermobile devices such as PDAs and mobile phones, whichmakes our TPM-based approach feasible for MANETs.

This mechanism provides a number of benefits, which make itsuitable for MANETs. First, policy enforcement in the multi-tier-networks is entirely distributed without relying on any centraltrusted choke points. Second, the trusted networks are self organized. They can be established and managed spontaneouslywithout requiring pre-deployed trusted entities or centralizedmanagement. Third, the multi-tier trust enables flexible enforcementof complex policies, which can be defined across variousinterdependent protocols and enforced independently, tier bytier. Furthermore, nodes running multiple applications can joinmultiple trusted networks, each enforcing policies for differentapplications without interfering with each other.We implemented a prototype of the policy enforcing mechanismin Linux and tested it over an IEEE 802.11-based wirelessad hoc network that is composed of TPM-enabled laptops. Wealso ran NS-2 simulations to evaluate the performance inlarge scale MANETs. The experimental results demonstrate lowoverall costs in application execution and network communicationdespite high one-time initial cost in network establishment.

The simulation results reveal that nodes can join the trusted tierswith high probability even if the underlying MANETs are highlyvolatile. The overall communication overhead over long network paths increases but still remains at low levels: less than 10% innetworks with infrequent connectivity loss and about 20% in highmobilitynetworks where connectivity among nodes is unstable.

Proposed Research

The policy social control mechanism resides on thehandheld device and ensures that the user adheres to thesecurity administrator's security policy settings nominativewithin a sound policy certificate keep on the device. Themechanism starts up because the device is initialized and checksthe issuer's signature on the policy certificate for authenticity, the well-formedness of the contents, andwhether the validation amount is in result. If a policycertificate isn't control or is found to be invalid, theenforcement mechanism applies a default policy havinglimited privileges.To ensure sure policy social control, we have a tendency to augment everynode with a sure agent, that protects the policyenforcement parts from being compromised. When anode joins a sure tier, its sure agent helps establish trustby proving the execution of an accurate sure agent, atrustworthy policy imposing software system part, and theright policy. Moreover, it ensures that the integrity of theagent, the help, and also the policy won't be compromised.This is potential as a result of the sure agent is a component of theoperating system kernel and guarantees the integrity of thekernel and every one programs concerned in policy social control.

III.METHODOLOGY

Phase 1: Using passive monitoring

During its first detection phase, the monitor conducts preliminary tests to detect collision occurrences in the wirelesschannel. the impact of physical and MAC layer jamming on the network measurements. The monitor uses the following metrics obtained from the physical and link layers to identify collisions.

1) Carrier Sensing Time: Based on 802.11 standard, every node in the wireless network performs physical carriersensing to sense the medium before transmission. When a malicious node attempts to continuously jam thewireless channel, the medium is always sensed busy for transmission. As a result, legitimate nodes in the network contending for channel access have a high carrier sensing duration. When the monitored nodes onan average have high carrier sensing time, it is possible that the region is being jammed. Carrier sensing time(Tcs) is thus used as an initial measure to indicate physical jamming conditions.

Test 1: PHY Jamming

if(Tcs>h)where η is an empirical threshold value obtained through simulation experiments.

2) Bit Errors: When a node experiences collision due to different signals received at the same time, it drops theframes due to bit errors. Although such error frames are not usually recorded, average number of bit errors can provide meaningful insights into the current state of collision in a wireless channel.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

Test 2: PHY/MAC Jamming
([E]) i if E e> ò
where E represents the acceptable value of bit errors in a wireless channel.

3) Frame retransmissions: Virtual Jamming attacks at the MAC layer causing collisions of RTS/CTS frames or DATA frames results in repeated retransmissions of the control or data frames respectively. Average number of frame retransmissions observed by the monitor node is an useful indicator of such collision attacks. The monitor runs the test to check if the average number of retransmissions of a node I (E[Ri])is greater than sum of the average number of retransmissions of all the other nodes in the network.

Test 3: MAC Jamming
If any of the above executed tests is true, it indicates the presence of a possible jamming attack in the network. Themonitor then calls phase 2 detection in order to confirm the detection.

Phase 2 :Using Cross-layer measurements
we address the challenge of reliably differentiating the collisions in the network caused either dueto jamming attacks or congested conditions. In this work, we propose a cross-layer based measurement driven approach where congestion estimation using physical, MAC and network layer measurements is used to identify collisions. Congestion estimation using channel utilization was presented in section 5. The monitor periodically runs jamming tests as well as evaluates the congestion status of the channel. Correlating results obtained from Phase I detection tests with estimated congestion level in the network facilitates accurate decision on jamming threats.

We outline the Phase detection algorithm below: Initially, we assume an optimistic network scenario andassign high confidence level to signify no jamming attacks. When any of the executed Phase I detection test results are true, the monitor node evaluates congestion state to check if the test results can be attributed to congested behaviour. If the network is highly congested, monitor determines jamming attack with high probability. Non-congested network scenarios combined with Phase I results indicate the presence of jamming with a high likelihood ratio. If however the network was moderately congested, Phase I results are alone not sufficient to detect jamming. In this case, we lower the confidence level in the network and repeat the detection algorithm after a duration interval D. Since the network confidence level is lowered any suspicious result when the process is repeated is classified as an attack. If a malicious node launches attack under congested network, it becomes more challenging to discern the cause of the network misbehaviour. In such cases, use of any rate adaptation algorithm to lower the bit rate in the network, can alleviate the effects of congestion. Decrease in bit rate lowers the congestion state and its impact on the network conditions. This enables better classification of jamming attacks from congested network behaviour.

Algorithm 2: Detection Algorithm
Initial Conditions: CONFIDENCE = HIGH;

Process:
if (Phase I test conditions TRUE) then
doCheckCongestionState()**;**
end if
CheckCongestionState()
if(Highly congested network) **then**
post no attack;
end if
if(Non congested network) **then**
post Jamming attack ;
end if
if(Moderately congested network) **then**
if(CONFIDENCE == LOW)
then
post Jamming attack ;
else
CONFIDENCE = LOW
repeat process after duration D;
end if
end if

IV. EXPERIMENTAL RESULTS

The simulation of the proposed method is done using ns-2, an open-source event-driven simulator for both wired and wireless networks. NS2 provides users with an executable command ns which takes on input argument, the name of a Tcl simulation scripting file. Users are feeding the name of a Tcl simulation script (which sets up a simulation) as an input argument of an NS2 executable command ns. In most cases, a simulation trace file is created, and is used to plot graph and/or to create animation. Simulation parameters are :

1) Grid size : 200 by 200 meters
2) Number of nodes : 10, 20, 50 mobile nodes (number of nodes varied)
3) Packet Traffic : CBR
4) Mobility : Random Way Point mobility model
5) Routing Protocol : AODV
6) MAC Layer : 802.11, peer-to-peer mode.
7) Radio : “no fading” radio model, with range of 376 meters.
8) Antenna : Omni-directional with unity gain
9) Simulation Time : 200 sec.

1) Jammer parameters -Jamming rate and distance of the jammer characterize the jammers behaviour. The rate at which the jammer transmits to launch collisions and the distance of jammer to the region directly affects the network degradation.

2) Malicious node ratio -The malicious node ratio represents the number of attackers in the network. Higher number of malicious nodes implies higher possibility of jamming.

3) Channel congestion rate -is defined as the rate of congestion estimated in the current channel. Highly

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

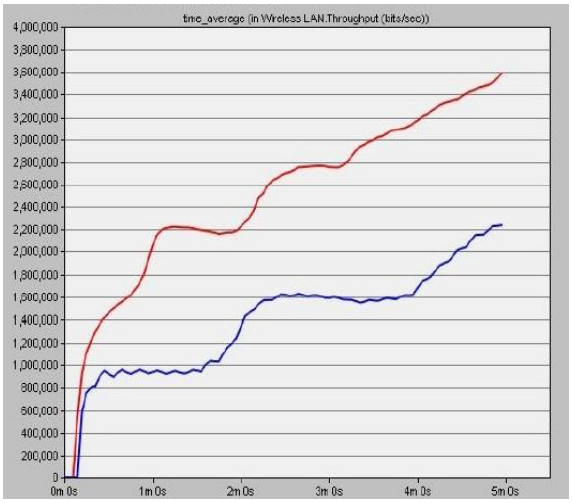
congested channel can lead to greater number of collisions increasing the false alarm rate in the network.

We propose the following metrics to evaluate the performance of our detection scheme:

- Detection rate: Detection rate measures the ratio of number of detected malicious collisions to the total number of collisions including undetected ones.
- False positive rate: False positives rate or the misalert rate measures the ratio of the number of detected collisions, due to channel congestion, to the total number of detected collisions.

The proposed method is implemented in the MAC layer of the 802.11 protocol in ns2. The simulation proceeds as follows. First, we simulated a network with 10 nodes organized into two clusters. Each cluster has a cluster head. It will periodically check the network for malicious behaviour. When one of the node in its neighbourhood act as a jammer, the cluster head identifies that node and broadcast a message to all the cluster nodes indicating the identity of the jammer node.

Then the neighbours will isolate the jammer node by denying service to it. The simulation is then extended for 20 and 50 nodes with number of clusters increased accordingly. Delivery ratio, overhead and energy consumed by the nodes are analysed. The same scenario is simulated with our proposed approach

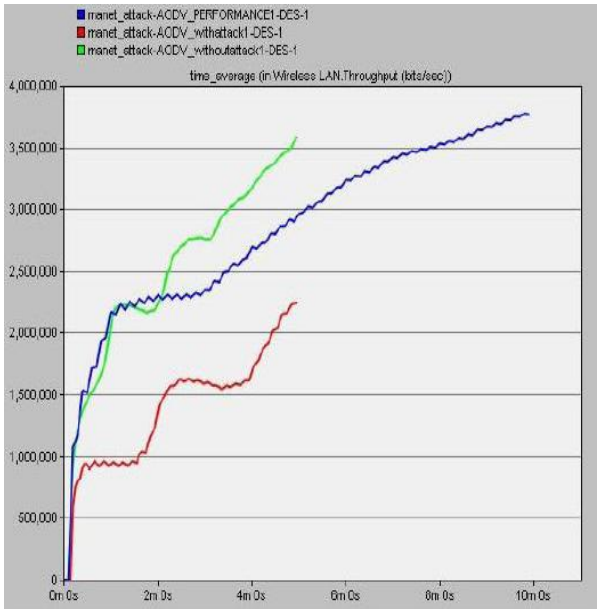


Detection of physical jamming attack

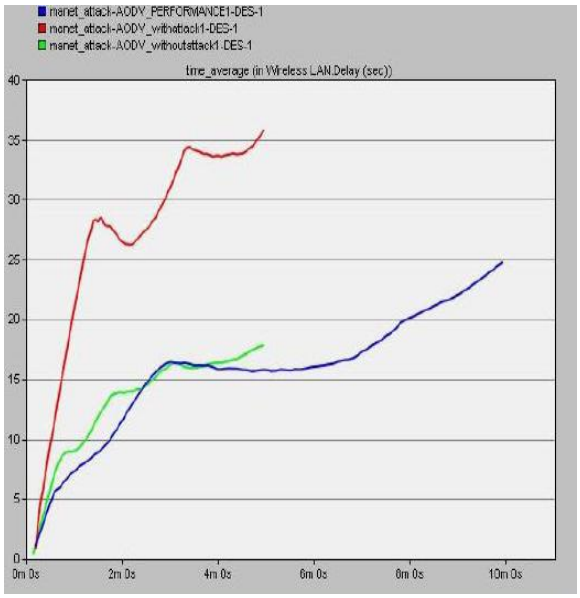
When the attack nodes were employed under AODV protocol into the network, then there is decrement in the network throughput thereby showing the existence of the physical jamming attack. Similarly, due the presence of attack in the network, the delay of the network increased.

Analysis of jamming attack under AODV protocol when the proposed technique was applied:

When the suggested mechanism was employed to the network of the mobile nodes in which the attack was detected, first the throughput of the network increased slowly and then arrived to a predicting level. On the other side, the net-work delay decreased to a significant value.



Throughput of the network under AODV with the Proposed Approach



Delay of the network with the proposed approach under AODV protocol

In the 20 nodes and 50 nodes network, till the beginning of the jammer activity, clustered approach shows greater delivery ratio. But during the jammer activity, LDS shows high performance. This implies that LDS can successfully deliver the packets in the presence of jammer by faster detection nd isolation of it from the network. the overhead of the clustered approach is drastically high after the occurrence of jamming activity. This is due to the resending of the packets when undelivered due to jamming attack. Once the network is initialized, the nodes began utilizing energy for transmission, reception and also broadcasting of messages. In the clustered approach, the nodes consume more energy than the LDS. Even in the presence of jamming activity, LDS shows a stable use of energy.

DOI 10.17148/IJARCCE.2016.5378

V.CONCLUSION

Mobile Adhoc Network (MANET) could be a system of wireless mobile nodes that dynamically self-organize in whimsical and temporary network topologies. The planned methodology can act as a Passive monitoring and cross layer measurement detection algorithms for distinguishing within jammers within the Manet. The analysis compares the performance of Passive monitoring and cross layer measurement detection algorithms organized network. electronic jamming attack mitigation and detection within the ad-hoc network mistreatment the algorithmic program by mistreatment delivery magnitude relation and signal strength is a smaller amount economical in passive observation. Delivery magnitude relation, overhead and energy square measure used as performance analysis metrics. although managing the name values creates somewhat overhead, it's really there in conjunction with a number of the routing protocols. By mitigating electronic jamming attacks, information measure utilization are often improved and thence rising the general network potency.

The work are often extended to incorporate some new, additional refined metrics for measure the potency of the electronic jamming attack and additionally for locating the sort of sender. If we will realize the sort of the sender, appropriate mechanisms are often developed for his or her identification and isolation.

We conclude that observation nodes square measure needed to forestall varied within and outdoors attacks. we tend to review the attack detection algorithmic program. In our work, we tend to propose new technique to isolate attack between the mobile nodes. we tend to implement new planned technique and compare the results with the previous techniques. Experimental Result shows that planned technique is healthier than existing technique.

Future Enhancement

For enhancing the turnout of the entire network, the existence of the sender node is extremely essential to be declared. Many techniques were most popular for determination, bar and removing of the ECM attack. so as to enhance the turnout and reduce the delay as compared of the offered techniques, associate degree improved detection technique is recommended during this paper, for sleuthing the physical ECM attack.

Future work conjointly specialize in observation nodes find malicious node that any doesn't send it to the destination. Therefore the nodes that find the malicious node reply to a supply node expect route node so supply isolates the trail and stop forwarding a lot of packets.

REFERENCES

[1]. Sisi Liu, LoukasLazos, and Marwan Krunz, "Thwarting Control-Channel Jamming Attacks from Inside Jammers," IEEE Transactions on mobile computing, vol. 11, pp. 1545–1558, September 2012

[2]. Karthikeyan U and Rajni ,"Security Issues Pertaining to Ad-Hoc Networks", International Journal for Research in Applied Science & Engineering Technology Volume 2 Issue XI, November 2014 ISSN: 2321-9653.

[3]. Gagandeep, Aashima and Pawan Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack- A Review," International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249-8958, Vol.1(5), June 2012

[4]. TajinderjitKaur and Sangeeta Sharma, "Mitigating the Impact of Jamming Attack by Using Antenna Patterns in MANET", VSRD-IJCSIT, Vol.2 (6), pp. 437-445, 2012

[5]. Le Wang and Alexander M.Wyglinski, "A combined approach for distinguishing different types of jamming attacks against wireless networks", proc. In Communications, Computers and Signal Processing (PacRim), 2011 IEEE Pacific Rim Conference, pp. 809-814.

[6]. RushaNandy, "Study of Various Attacks in MANET and Elaborative Discussion Of Rushing Attack on DSR with clustering scheme" Int. J. Advanced Networking and Applications Volume: 03, Issue: 01, Pages:1035-1043 (2011)

[7]. PranitaChaudhar, C. RamaKrishna and SasmitaBehera, "A Review on Packet-Hiding Methods to Hamper Selective Jamming Attacks in wireless networks", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 8 August, 2013 Page No. 2377-2387

[8]. NischayBahl, Ajay K. Sharma and Harsh K. Verma "Impact of Physical Layer Jamming on Wireless Sensor Networks with Shadowing and Multicasting" I. J. Computer Network and Information Security, 2012.

[9]. Arif Sari, ―Security Approaches in IEEE 802.11 MANET-Performance Evaluation of USM and RASǁ, in IJCNS International Journal of Communica-tions, Network and System Sciences, 7, 365-372, 2014.

[10]. NadeemSufyan, NazarAbbassSaqib, Muhammad Zia ― Detection of jamming attack in 802.11b wireless networksǁ, in EURASIP Journal on Wireless Communications and Networking, 2013.

DOI 10.17148/IJARCCE.2016.5378