Overview on Network Security and its Vulnerabilities

[1]S.Fathima, [2]Dr.S.Karthik, [3]R.M.Bhavadharini

[1]PG Scholar, Department of Computer Science and Engineering, SNS College of Technology, Coimbatore, TamilNadu. India.
[2]Professor & Dean, Department of Computer Science and Engineering, SNS College of Technology, Coimbatore, TamilNadu. India.
[3]Assistant Professot (SG), Department of Computer Science and Engineering, SNS College of Technology, Coimbatore, TamilNadu. India.

***Abstract*--**In this paper, we talk about security issues and their current results in the versatile specially appointed system. Mobile ad hoc network can be defined as a collection of mobile nodes which can be useful for form a network without help existing network. Nodes in network act as host and router which is used for send the packets for other device. The nature of MANET's are dynamic topology, node mobility, scalability, self organizing capability is lead the network. Many security threats that disturb the open and distributed communication development which is challenging task .We first break down the primary vulnerabilities in the portable mobile ad hoc networks, which have made it much simpler to experience the ill effects of assaults than the conventional wired system. At that point we talk about the security criteria of the portable mobile ad hoc network what's more present the principle assault sorts that exist in it. At last we overview the current security answers for the portable specially appointed system.

Key Words: *Mobile Ad Hoc Network, Security, Intrusion Detection*

*****

1. INTRODUCTION:

In recent years, the explosive growth of mobile computing devices, that in the main embody Laptops, personal digital assistants (PDAs) and hand-held digital devices, has driven a Revolutionary amendment within the computing world: computing won't just have faith in the Capability provided by the private computers, and therefore the construct of present computing Emerges and becomes one amongst the analysis hotspots within the engineering science society [1]. In the ubiquitous computing setting, individual users utilize, at a similar time, several electronic platforms through that they will access all the specified information whenever and wherever they'll be [2]. The character of the ever present computing has created it necessary to adopt wireless network because the interconnection method: it's impracticable for the ever present devices to urge wired network link whenever and where they have to attach with alternative ubiquitous devices. The Mobile unexpected Network is one amongst the wireless networks that have attracted most concentrations from several researchers.

A Mobile adhoc Network (MANET) could be a system of wireless mobile nodes that dynamically Self-organize in capricious and temporary network topologies. Folks and vehicles will therefore be internetworked in areas while not a preceding communication infrastructure or once the utilization of such infrastructure needs wireless extension [3]. Within the mobile unexpected network, nodes

can directly communicate with all the opposite nodes among their radio ranges; whereas nodes that not within the direct communication vary use intermediate node(s) to speak with each other. In these 2 things, all the nodes that have participated within the communication Automatically kind a wireless network, so this sort of wireless network may be viewed as mobile unexpected network.

The mobile unexpected network has the subsequent typical options [4]:

- Undependableness of wireless links between nodes. Attributable to the restricted energy offer for the wireless nodes and therefore the quality of the nodes, the wireless links between mobile nodes within the unexpected network aren't consistent for the communication participants.
- Perpetually ever-changing topology. Thanks to the continual motion of nodes, the topology of the mobile unexpected network changes constantly: the nodes will unceasingly get into and out of the radio vary of the opposite nodes within the unexpected network, and therefore the routing information are ever-changing all the time attributable to the movement of the nodes.
- Lack of incorporation of safety features in statically organized wireless routing protocol not meant for unexpected environments. as a result of the topology of the unexpected networks is ever-changing perpetually, it's necessary for every combine of adjacent nodes to incorporate within the routing issue thus on stop some reasonably potential attacks that attempt to make use of vulnerabilities within the statically organized routing protocol.

Because of the options listed higher than, the mobile unexpected networks square measure a lot of liable to suffer from the malicious behaviors than the standard wired networks. Therefore, we want to pay more attention to the protection problems within the mobile unexpected networks.

2. Vulnerabilities of the Mobile unintended Networks

Because mobile unintended networks have way more vulnerabilities than the normal wired networks, security is way tougher to keep up within the mobile unintended network than within the wired network. During this section, we tend to discuss the varied vulnerabilities that exist within the mobile ad hoc networks.

2.1. Lack of Secure Boundaries

The means of this vulnerability is self-evident: there's not such a transparent secure boundary in The mobile unintended network, which may be compared with the cleared line of defense within the Traditional wired network. This vulnerability originates from the character of the mobile unintended Network: freedom to affix, leave and move within the network.

In the wired network, adversaries should get physical access to the network medium, or even pass through many lines of defense like firewall and entryway before they'll perform Malicious behavior to the targets [6]. However, within the mobile unintended network, there's no would like for associate degree person to realize the physical access to go to the network: once the person is within the radio vary of the other nodes within the mobile unintended network, it will communicate with those nodes in its radio vary and therefore be pared of the network mechanically. As a result, the mobile ad hoc network doesn't offer the alleged secure boundary to safeguarded the network from some Potentially dangerous network accesses. Lack of secure boundaries makes the mobile unintended network at risk of the attacks. The mobile unintended network suffers from unrestricted attacks, which may come back from any node that is within the radio vary of any node within the network, at any time, and target to the other node(s) in the network. To form matters worse, there square measure numerous link attacks that may jeopardize the mobile unintended network, that create it even tougher for the nodes within the network to resist the attacks. The attacks in the main embody passive eavesdropping, active busybodies, leakage of secret info, information change of state, message replay, message contamination, and denial of service [4].

2.2. Threats from Compromised nodes within the Network

In the previous section, we tend to in the main discuss the vulnerability that there's no cleared secure boundaries within the mobile unintended network, which can cause the occurrences of varied link attacks. These link attacks place their stress on the links between the nodes, and try to perform some malicious behaviors to form destruction to the links. However, there square measure some other attacks that aim to realize the management over the nodes themselves by some evil means so use the compromised nodes to execute additional malicious actions. This vulnerability are often viewed because the threats that come back from the compromised nodes within the network.

Since mobile nodes square measure autonomous units that may be pared of or leave the network with freedom, it is hared for the nodes themselves to figure out some effective policies to stop the attainable malicious behaviors from all the nodes it communicate with due to the activity diversity of various nodes. moreover, due to the quality of the unintended network, a compromised node will oft modification its attack target and perform malicious behavior to different node within the network, therefore it's terribly tough to trace the malicious behavior performed by a compromised node particularly in a very giant scale unintended network. Therefore, threats from compromised nodes within the network square measure way more dangerous than the attacks from outside the network, and these attacks square measure a lot of tougher to observe as a result of they are available from the compromised nodes, that behave well before they're compromised. A good example of this sort of threats comes from the potential Byzantine failures encountered within the routing protocol for the mobile unintended network [4]. we tend to decision it a Byzantine failure once a group of nodes square measure compromised in such the simplest way that the inaccurate and malicious behavior can't be directly detected due to the cooperation among these compromised nodes once they perform malicious behaviors. The compromised nodes could on the face of it behave well; but, they'll truly create use of the failings and inconsistencies within the routing protocol to undetectably destroy the routing material of the network, generate and advertise new routing info that contains nonexistent link, offer pretend link state information, or maybe flood alternative nodes with routing traffic. as a result of the compromised nodes cannot be simply recognized, their malicious behaviors square measure vulnerable to be unheeded by alternative nodes.

Therefore Byzantine failure is extremely harmful to the mobile unintended network.

From on top of we discover that the threats from compromised nodes within the unintended network should be paid a lot of attention, and mobile nodes and infrastructure shouldn't simply trust any node within the network though it behaves well before as a result of it'd are compromised.

2.3. Lack of Centralized Management Facility

Ad hoc networks don't have a centralized piece of management machinery like a reputation server, that cause some vulnerable issues. Currently allow us to discuss this drawback in a very a lot of Detailed manner.

First of all, the absence of centralized management machinery makes the detection of attacks a very tough drawback as a result of it's tough to observe the traffic in a very extremely dynamic and large scale unintended network [7]. it's rather common within the unintended network that benign failures, such as path breakages, transmission impairments and packet dropping, happen oft.

Therefore, malicious failures are going to be tougher to observe, particularly once adversaries change their attack pattern and their attack target in several periods of your time. for every of the victims, as a result of it will solely observe the failure that happens in itself, this short-time Observation cannot turn out a convincing conclusion that the failure is caused by associate degree person.

However, we will simply realize from a system purpose of read that the person has performed such an oversized quantity of misbehaviors that we will safely conclude that every one of the failures caused by this person ought to be malicious failure rather than benign failure, though these failures occur completely different in frequent nodes at different time. From this instance we discover that lack of centralized management machinery can cause severe issues once we attempt to observe the attacks within the unintended network.

Second, lack of centralized management machinery can impede the trust management for the nodes within the unintended network [4]. In mobile unintended network, all the nodes square measure needed to cooperate within the network operation, whereas no security association (SA2) are often assumed for all the network nodes. Thus, it's not sensible to perform associate degree a priori classification, and as a result, the standard apply of building a line of defense, that distinguishes nodes as sure and no trusted, can't be achieved here within the mobile unintended network.

Third, some algorithms within the mobile unintended network have confidence the cooperative participation of all nodes and therefore the infrastructure. as a result of there's no centralized authority, and decision-making in mobile unintended network is typically decentralized, the person will create use of this vulnerability and perform some attacks that may break the cooperative algorithmic program [6].

In one word, the absence of centralized management machinery can cause vulnerability that can influence many aspects of operations within the mobile unintended network. Therefore we must always work out some solutions to traumatize this drawback, which could be mentioned within the later section.

2.4. Restricted Power offer

As we tend to all recognize, owing to the quality of nodes within the unintended network, it's common that the nodes within the unintended network can replay on battery as their power offer methodology. whereas nodes in the wired network don't got to take into account the ability offer drawback as a result of they'll get electric power offer from the shops, that typically mean that their power offer ought to be around infinite; the nodes within the mobile unintended network got to take into account the restricted battery power, which is able to cause many issues.

The first drawback which will be caused by the restricted power offer is denial-of-service attacks [4]. Since the person is aware of that the target node is battery-restricted, either it will continuously send extra packets to the target and raise it routing those extra packets, or it will induce the target to be cornered in some quite long computations. In this way, the battery power of the target node are going to be exhausted by these insignificant tasks, and thus the target node are going to be out of service to any or all the benign service requests since it's run out of power.

Furthermore, a node within the mobile unintended network could behave in a very ungenerous manner once it finds that there's solely restricted power offer, and therefore the stinginess will cause some issues when there's a requirement for this node to get together with alternative nodes to support some functions in the network. simply take the cluster-based intrusion detection technique as associate degree example [8]. In this technique, there's no would like that each node within the unintended network is that the watching node all the time; instead, a cluster of neighboring Eduard Manet nodes will at random and fairly elect a monitoring node which will observe the abnormal behaviors within the network traffic for the whole cluster. However, a very important precondition for the success of this method is that each node within the cluster is willing to require their responsibility as a watching node and serve for all other nodes in a very amount of your time. There is also some nodes that behave egotistically and don't want to get together within the watching node election method, which is able to create the election fail if there square measure too several ungenerous nodes. Moreover, we must always not read all of the ungenerous nodes as malicious nodes: some nodes could encounter restricted power offer drawback and therefore behave in a very ungenerous manner, which may be tolerated; but, there are often another node who by choice announces that it runs out of battery power and thus don't wish to cooperate with alternative nodes in some cooperative operation, however truly this node still has enough battery power to support the cooperative operation.

In a word, ungenerous behaviors should not be thought to be malicious behaviors, however we want to understand if the stinginess is basically caused by the restricted battery power, or by the intentional non-cooperation.

2.5. Quantifiability

Finally, we want to deal with the quantifiability drawback once we discuss the vulnerabilities within the mobile unintended network [4]. in contrast to the normal wired network in this its scale is usually predefined once it's designed and cannot modification a lot of throughout the utilization, the size of the ad hoc network keeps ever-changing all the time: due to the quality of the nodes within the mobile ad hoc network, you'll hardly predict what number nodes there'll be within the network within the future. As a result, the protocols and services that square measure applied to the unintended network like routing protocol and key management service ought to be compatible to the endlessly changing scale of the unintended network, which can vary from decades of nodes to many nodes, or maybe thousands of nodes. In alternative words, these protocols and services got to scale up and down expeditiously.

2.6. Vulnerabilities of the Mobile unintended Networks: Summary

From the discussion during this section, we will safely conclude that the mobile unintended network is insecure by its nature: there's no such a transparent line of defense due to the liberty for the nodes to affix, leave and move within the network; a number of the nodes is also compromised by the person and therefore perform some malicious behaviors that square measure exhausting to detect; lack of centralized machinery could cause some issues once there's a requirement to own such a centralized coordinator; restricted power offer will cause some ungenerous problems; and continuously ever-changing scale of the network has set higher demand to the quantifiability of the protocols and services within the mobile unintended network. As a result, compared with the wired network, the mobile unintended network can would like a lot of sturdy security theme to confirm the security of it. Within the next section, we are going to survey security attacks that may helpful to identify the intrusion among nodes.

3. Attack varieties in Mobile ad hoc spatial Networks

There are various forms of attacks within the mobile accidental network, the majority of which may be classified because the following 2 varieties [6]:

(i). External attacks, within which the aggressor aims to cause congestion, propagate pretend routing information or disturb nodes from providing services.

(ii). Internal attacks, within which the mortal desires to achieve the conventional access to the network and participate the network activities, either by some malicious impersonation to urge the access to the network as a brand new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors.

In the 2 classes shown higher than, external attacks are kind of like the conventional attacks within the traditional wired networks in this the mortal is within the proximity however not a sure node in the network, therefore, this kind of attack are often prevented and detected by the safety methods like membership authentication or firewall, that are comparatively typical security solutions. However, because of the pervasive communication nature and open network media within the mobile accidental network, internal attacks are way more dangerous than the interior attacks: as a result of the compromised nodes are originally the benign users of the accidental network, they can simply pass the authentication and acquire protection from the safety mechanisms. As a result, the adversaries will build use of them to achieve traditional access to the services that ought to only be on the market to the approved users within the network, and that they will use the legal identity provided by the compromised nodes to hide their malicious behaviors. Therefore, we should pay a lot of attention to the interior attacks initiated by the malicious insiders after we consider the safety problems within the mobile accidental networks. Within the following, we have a tendency to discuss the main attack varieties that emerge within the mobile accidental networks.

3.1. Denial of Service (Dos)

The first kind of attack is denial of service, that aims to crab the supply of sure node or even the services of the whole accidental networks. Withal, it becomes not sensible to perform the normal Dos attacks in the mobile accidental networks due to the distributed nature of the services. Moreover, the mobile accidental networks are a lot of vulnerable than the wired networks due to the Interference-prone radio channel and therefore the restricted battery power. Within the apply, the attackers exactly use the radio jam and battery exhaustion ways to conduct DoS attacks to the mobile accidental networks, that well correspond to the 2 vulnerabilities.

3.2. Impersonation

Impersonation attack may be a severe threat to the safety of mobile accidental network [4]. As we can see, if there's not such a correct authentication mechanism among the nodes, the adversary will capture some nodes within the network and build them appeared as if benign nodes. In this way, the compromised nodes will be a part of the network because the traditional nodes and start to conduct the malicious behaviors like propagate pretend routing info and gain inappropriate priority to access some direction.

3.3. Eavesdropping

Eavesdropping is another quite attack that typically happens within the mobile accidental networks.

The goal of eavesdropping is to get some direction that ought to be unbroken secret throughout the communication. The direction might embody the situation, public key, non-public key or perhaps passwords of the nodes. as a result of such information are vital to the safety state of the nodes, they ought to be unbroken fare from the unauthorized access.

3.4. Attacks Against Routing

Routing is one in every of the foremost necessary services within the network; so it's additionally one in every of the main targets to that attackers conduct their malicious behaviors. within the mobile accidental networks, attacks against routing are typically classified into 2 categories: attacks on routing protocols and attacks on packet forwarding/delivery [6]. Attacks on routing protocols aim to dam the propagation of the routing info to the victim albeit there are some routes from the victim to alternative destinations. Attacks on packet forwarding try and disturb the packet delivery on a predefined path.

The main influences brought by the attacks against routing protocols embody network partition, routing loop, resource deprivation and route hijack [6]. There are some attacks against routing that are studied and standard [10] [11] [12] [13]:

- Impersonating another node to spoof route message.
- Advertising a false route metric to misrepresent the topology.
- causing a route message with wrong sequence variety to suppress alternative legitimate route messages.
- Flooding Route Discover overly as a DoS attack.
- Modifying a Route Reply message to inject a false route.
- Generating imitative Route Error to disrupt a operating route.
- Suppressing Route Error to mislead others.

Because of the quality and perpetually dynamic topology of the mobile accidental networks, it is very troublesome to validate all the route messages [6]. There are some a lot of refined routing attacks, that embody hole attacks [14], dashing attacks [15] and Sybil attacks [16].

The second class of attacks against routing is attacks on packet forwarding/delivery, which aren't simple to notice and prevented [6]. There are 2 main attack ways during this type: one is stinginess, within which the malicious node by selection drops route messages that are assumed to forward so as to save lots of it own battery power; the opposite is denial-of-service, in which the mortal sends out overwhelming network traffic to the victim to exhaust its battery power.

3.5. Attack varieties in Mobile accidental Networks: Summary

In this half, we have a tendency to principally discuss the attack varieties within the mobile accidental networks. The attacks in MANET are often in brief classified into 2 categories: external attacks and internal attacks, latter of that are way more dangerous to the mobile accidental network. Then we have a tendency to in brief introduce the most attack varieties within the mobile accidental network, that are denial-of-service(DoS) attacks, impersonation attacks, eavesdropping attacks and attacks against routing. In the next section, we are going to survey many standard security solutions to the attacks mentioned above.

3.Security Solutions to the Mobile ad hoc spatial Networks

C if we tend to simply recognize the prevailing vulnerabilities in it. As a result, we need to find some security solutions to the mobile ad hoc spatial network. During this section, we tend to survey some security schemes which will be helpful to safeguard the mobile ad hoc spatial network from malicious behaviors are,

3.1. Security Criteria

Before we tend to survey the solutions which will facilitate secure the mobile ad hoc spatial network, we expect it necessary to search out however we are able to choose if a mobile ad hoc spatial network is secure or not, or in other words, what ought to be lined within the security criteria for the mobile ad hoc spatial network when we need to examine the safety state of the mobile ad hoc spatial network. within the following, we briefly introduce the widely-used criteria to gauge if the mobile ad hoc spatial network is secure.

3.1.1. Convenience

The term convenience means a node ought to maintain its ability to supply all the designed services in spite of the safety state of it [4]. This security criterion is challenged primarily during the denial-of-service attacks, within which all the nodes within the network are often the attack target and so some stingy nodes build a number of the network services untouchable, such as the routing protocol or the key management service [5].

3.1.2. Integrity

Integrity guarantees the identity of the messages once they square measure transmitted. Integrity are often compromised primarily in 2 ways that [9]:

- Malicious fixing
- Accidental fixing

A message are often removed, replayed or revised by Associate in Nursing somebody with malicious goal, which is regarded as malicious altering; on the contrary, if the message is lost or its content is modified due to some failures, which can be transmission errors in communication

or hardware errors like magnetic disc failure, then it's classified as accidental fixing.

3.1.3. Confidentiality

Confidentiality means sure info is barely accessible to those that are authorized to access it. In different words, so as to take care of the confidentiality of some confidential info, we'd like to stay them secret from all entities that don't have the privilege to access them.

3.1.4. Credibility

Authenticity is actually assurance that participants in communication square measure real and not impersonators [4]. it's necessary for the communication participants to prove their identities as what they need claimed victimization techniques soon make sure the credibility. If there's not such associate in nursing authentication mechanism, the somebody may impersonate a benign node and thus get access to confidential resources, or maybe propagate some faux messages to disturb the normal network operations.

3.1.5. Non repudiation

Non repudiation ensures that the sender and therefore the receiver of a message cannot deny that they have ever sent or received such a message. this can be helpful particularly once we got to discriminate if a node with some abnormal behavior is compromised or not: if a node recognizes that the message it's received is inaccurate, it will then use the wrong message as associate in nursing proof to apprize different nodes that the node causing out the improper message ought to have been compromised.

3.1.6. Authorization

Authorization could be a method within which Associate in Nursing entity is issued a papers, that specifies the privileges and permissions it's and can't be falsified, by the certificate authority. Authorization is usually accustomed assign totally access rights to different level of users. For instance, we'd like to confirm that network management operate is barely accessible by the network administrator. thus there ought to be Associate in Nursing authorization method before the network administrator accesses the network management functions.

3.1.7. Anonymity

Anonymity means all the knowledge which will be accustomed establish the owner or this user of the node ought to default be unbroken personal and not be distributed by the node itself or the system software package. This criterion is closely associated with privacy conserving, within which we must always try to defend the privacy of the nodes from arbitrary speech act to the other entities.

3.1.8. Security Criteria: outline

We have mentioned many main needs that require to be achieved to confirm the safety of the mobile ad hoc spatial network. Moreover, there square measure another security criteria that square measure additional specialized and application-oriented, that embrace location privacy, self-stabilization and Byzantine strength, all of that square measure associated with the routing protocol within the mobile ad hoc spatial network. Having controlled the most security criteria, we tend to then move to the discussion on the main threats that violate the safety criteria, that square measure typically known as attacks.

4. CONCLUSION:

In this survey paper, we have a tendency to attempt to examine the protection problems within the mobile ad hoc networks, which may be a main disturbance to the operation of it. As a result of the quality and open media nature, the mobile ad hoc spatial networks are far more vulnerable to all quite security risks, such as information revelation, intrusion, or maybe denial of service. As a result, the protection wants in the mobile ad hoc spatial networks are abundant over those within the ancient wired networks.

First we have a tendency to in short introduce the fundamental characteristics of the mobile ad hoc network. Because of the emergence of the thought pervasive computing, there's associate degree increasing would like for the network users to urge reference to the planet anytime at anyplace, that evokes the emergence of the mobile ad hoc network. However, with the convenience that the mobile ad hoc networks have delivered to North American nation, there also are increasing security threats for the mobile ad hoc network, which require realizing enough attention. We then discuss some typical and dangerous vulnerability within the mobile ad hoc networks, most of that are caused by the characteristics of the mobile ad hoc spatial networks like mobility, perpetually dynamic topology, open media and restricted battery power. The existence of these vulnerabilities has created it necessary to search out some effective security solutions and protect the mobile ad hoc network from every kind of security risks. Finally we have a tendency to introduce the present security solutions for the mobile ad hoc networks. We start with the discussion on the protection criteria in mobile ad hoc network, that acts as a steerage to the security-related analysis works during this space. Then we have a tendency to point out the most attack varieties that threaten the present mobile ad hoc networks. In the end, we have a tendency to discuss many security techniques that may facilitate defend the mobile ad hoc networks from external and internal security threats. During the survey, we have a tendency to additionally notice some points that may be additional explored within the future, such as the intrusion detection techniques will get additional improvement.

Reference

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[15] Y. Hu, A. Perrig and D. Johnson, Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols, in *Proceedings of ACM MobiCom Workshop - WiSe'03,* 2003.

[16] J. R. Douceur, The Sybil Attack, in *Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS'02),* pages 251–260, March 2002, LNCS 2429.

[17] Intrusion-detection system, from *Wikipedia, the free encyclopedia*, http://en.wikipedia.org/wiki/Intrusion-detection_system.

[18] Y. Zhang and W. Lee, Intrusion Detection in Wireless Ad-hoc Networks, in *Proceedings of the 6th International Conference on Mobile Computing and Networking (MobiCom 2000)*, pages 275–283, Boston, Massachusetts, August 2000.

[19] Jim Parker, Anand Patwardhan, and Anupam Joshi, Detecting Wireless Misbehavior through Cross-layer Analysis, in *Proceedings of the IEEE Consumer Communications and* 23 *Networking Conference Special Sessions (CCNC'2006),* Las Vegas, Nevada, 2006.

[20] P. Krishna, N. H. Vaidya, M. Chatterjee and D. K. Pradhan, A Cluster-based Approach for Routing in Dynamic Networks, *ACM SIGCOMM Computer Communication Review*, 27(2):49–64, 1997.