Journal of Advances in Science and Technology

Vol. IX, Issue No. XIX, May-2015, ISSN 2230-9659

# NEW HOPE AND SECURITY ISSUES OF WIRELESS AD HOC NETWORKS: A COMPREHENSIVE STUDY

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

www.ignited.in

*Journal of Advances in Science and Technology*
*Vol. IX, Issue No. XIX, May-2015, ISSN 2230-9659*

# New Hope and Security Issues of Wireless Ad Hoc Networks: A Comprehensive Study

**S. Avidaiappan**

Research Scholar, Directorate of Distance and Continuing Education, Manonmaniam Sundaranar University

***Abstract – In this paper we discuss about the improvement of security and privacy issues in wireless Ad-hoc network, wireless mesh network and wireless sensor network with the help of routing protocols, authentication and cryptographic tools. Ad hoc network is a collection of nodes that is connected through a wireless medium forming rapidly changing topologies. Attacks on ad hoc network routing protocols disrupt network performance and reliability with their solution. We briefly present the most popular protocols that follow the table-driven and the source-initiated on-demand approaches. The comparison between the proposed solutions and parameters of ad hoc network shows the performance according to secure protocols. We discuss in this paper routing protocol and challenges and also discuss authentication in ad hoc network.***

***With the advancement in radio technologies like Bluetooth, IEEE 802.11, a new concept of networking has emerged; this is known as ad hoc networking where potential mobile users arrive within the range for communication. As network is becoming an increasingly important technology for both military and commercial distributed and group based applications, security is an essential requirement in mobile ad hoc network (MANETs). Compared to wired networks, MANETs are more vulnerable to security attacks due to the lack of a trusted centralized authority and limited resources. Attacks on ad hoc networks can be classified as passive and active attacks or internal attack and external attacks, the security services such as confidentiality, authenticity and data integrity are also necessary for both wired and wireless networks to protect basic applications. One main challenge in design of these networks is their vulnerability to security attacks.***

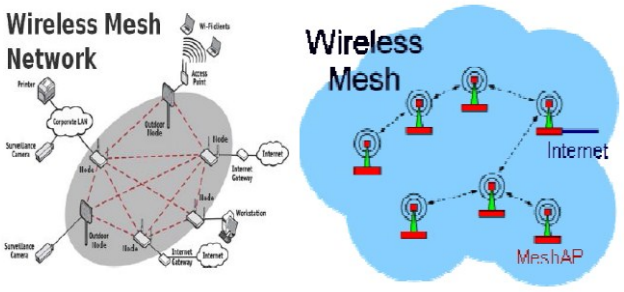
----------♦----------

## INTRODUCTION

A wireless ad hoc network is a decentralized type of wireless network. The network is ad hoc because it does not rely on a pre-existing 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, so the determination of which nodes forward data is made dynamically on the basis of network connectivity.

In addition to the classic routing, ad hoc networks can use flooding for forwarding data. An ad hoc network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other ad hoc network device in link range. Ad hoc network often refers to a mode of operation of IEEE 802.11 wireless networks. This paper provides insight into the potential applications of ad hoc networks and discusses the Technological challenges that protocol designers and network developers are faced with. These challenges include routing, service and resource discovery, Internet connectivity, Billing and security. Most recent ad hoc network research has focused on providing routing services without considering security.

Wireless mesh networking has emerged as a promising technology to meet the challenges of the next generation wireless communication networks for providing flexible, adaptive, and reconfigurable architecture and offering cost-effective business solutions to the service providers. The potential applications of wireless mesh networks (WMNs) are wide-ranging such as: backhaul connectivity for cellular radio access networks, high-speed wireless metropolitan area networks (WMANs), community networking, building automation, intelligent transportation system (ITS) networks, defense systems, and city-wide surveillance systems etc. Although several architectures for WMNs have been proposed based on their applications, the most generic and widely accepted one is a three tier structure as depicted in Figure.




Wireless Sensor Networks (WSN) is an emerging technology and day by day it is attracting the attention of researchers with its challenging characteristics and diversified application domain. The more researchers try to develop further cost and energy efficient computing devices and algorithms for WSN, the more challenging it becomes to fit the security of WSN into that constrained environment. However, security is crucial to the success of applying WSN. So, familiarity with the security aspects of WSN is essential before designing WSN system. This paper studies the security problems of WSN based on its resource restricted design and deployment characteristics and the security requirements for designing a secure WSN. Also, this study documents the well-known attacks at the different layers of WSN and some counter measures against those attacks. Finally, this paper discusses on some defensive measures of WSN giving focus on the key management, link layer and routing security.

Research on Wireless Ad Hoc Networks has been ongoing for decades. The history of wireless ad hoc networks can be traced back to the Defense Advanced Research Project Agency (DAPRPA) packet radio networks (PRNet), which evolved into the survivable adaptive radio networks (SURAD) program. Ad hoc networks have play an important role in military applications and related research efforts, for example, the global mobile information systems (GloMo) program and the near-term digital radio (NTDR) program. Recent years have seen a new spate of industrial and commercial applications for wireless ad hoc networks, as viable communication equipment and portable computers become more compact and available.

Since their emergence in 1970's, wireless networks have become increasingly popular in the communication industry. These networks provide mobile users with ubiquitous computing capability and information access regardless of the users' location. There are currently two variations of mobile wireless networks: infrastructure and infrastructure less networks.

The infrastructure networks have fixed and wired gateways or the fixed Base-Stations which are connected to other Base-Stations through wires. Each node is within the range of a Base-Station. A "Hand-off" occurs as mobile host travels out of range of one Base-Station and into the range of another and thus, mobile host is able to continue communication seamlessly throughout the network. Example applications of this type include wireless local area networks and Mobile Phone.

The other type of wireless network, infrastructure less networks, is knows as Mobile Ad-hoc Networks (MANET). These networks have no fixed routers, every node could be router. All nodes are capable of movement and can be connected dynamically in arbitrary manner.

The responsibilities for organizing and controlling the network are distributed among the terminals themselves.

The entire network is mobile, and the individual terminals are allowed to move freely. In this type of networks, some pairs of terminals may not be able to communicate directly with each other and have to rely on some terminals so that the messages are delivered to their destinations. Such networks are often referred to as multi-hop or store-and forward networks. The nodes of these networks function as routers, which discover and maintain routes to other nodes in the networks. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices.

Mobile Ad-hoc Networks are supposed to be used for disaster recovery, battlefield communications, and rescue operations when the wired network is not available. It can provide a feasible means for ground communications and information access.

## LITERATURE REVIEW

Wireless networks consist of a number of nodes which communicate with each other over a wireless channel which have various types of networks: sensor network, ad hoc mobile networks, cellular networks and satellite networks. Wireless sensor networks consist of small nodes with sensing, computation and wireless communications capabilities. Many routing protocols have been specifically designed for WSNs where energy awareness is the key issue. Routing protocols

in WSNs differ depending on the application and network architecture. Ad-hoc networks are a new paradigm of wireless communication for mobile hosts where node mobility causes frequent changes in topology. Ad hoc networks are self-configurable and autonomous systems consisting of routers and hosts, which are able to support movability and organize themselves arbitrarily.

This means that the topology of the ad hoc network changes dynamically and unpredictably. Moreover, the ad hoc network can be either constructed or destructed quickly and autonomously without any administrative server or infrastructure. Without support from the fixed infrastructure, it is undoubtedly

arduous for people to distinguish the insider and outsider of the wireless network. That is to say, it is not easy for us to tell apart the legal and the illegal participants in wireless systems. Because of the above mentioned properties, the implementation of security infrastructure has become a critical challenge when we design a wireless network system. If the nodes of ad hoc networks are mobile and with wireless communication to maintain the connectivity, it is known as mobile ad hoc network (MANET) and require an extremely flexible technology for establishing communications in situations which demand a fully decentralized network without any fixed base stations, such as battlefields, military applications, and other emergency and disaster situations.

A MANET is a most promising and rapidly growing technology which is based on a self-organized and rapidly deployed network. Due to its great features, MANET attracts different real world application areas where the networks topology changes very quickly. However, in many researchers are trying to remove main weaknesses of MANET such as limited bandwidth, battery power, computational power, and security. Although a lot of work under progress in this subject particularly routing attacks and its existing countermeasures. The existing security solutions of wired networks cannot be applied directly to MANET, which makes a MANET much more vulnerable to security attacks. In this paper, we have discussed current routing attacks in MANET.

Some solutions that rely on cryptography and key management seem promising, but they are too expensive for resource constrained in MANET. They still not perfect in terms of tradeoffs between effectiveness and efficiency. Some solutions in work well in the presence of one malicious node, they might not be applicable in the presence of multiple colluding attackers. In addition, some may require special hardware such as a GPS or a modification to the existing protocol.

The malicious node(s) can attacks in MANET using different ways, such as sending fake messages several times, fake routing information, and advertising fake links to disrupt routing operations.

Stephen Michell, et al., (2004) proposed state based key hope protocol (SBKH) that provides a lightweight encryption scheme for battery operated devices such as the sensors in a wireless sensor network as well as small office, home office (SOHO) users. State based key hope protocol implements encryption in a novel state based way so as to provide cheap and robust security without additional overheads of encryption. Implementation of SBKH on real hardware is a challenge.

Gamal Selim, et al., (2006) explained various types of security attacks modification, fabrication, interception, brute force, maintainability and static placement of MIC. They surveyed currently available security protocols i.e. WEP, WEP2, WPA and WPA2. They also proposed a new mechanism called multiple slot system (MSS). MSS makes use of the key selector, slot selector and MIC shuffle selector. MSS uses one of four encryption algorithm RC4, RSA, Blowfish and AES.

Andrew Gin, et al., (2008) compared the performance analysis of evolving wireless 802.11 security architecture. Paper explained wireless network security methods. Paper explained security layers like WEP shared key authentication and 40 bit encryption, WEP shared key authentication and 104 bit encryption, WPA with PSK authentication and RC4 encryption, WPA with EAP-TLS authentication and RC4 encryption, WPA2 with PSK authentication and AES encryption and WPA2 with EAP-TLS authentication and AES encryption. Effects on throughput are also discussed.

Arash Habibi Lashkari, et al., (2009) presented a survey on wireless security protocols (WEP, WPA and WPA2/802.11i). Here WEP protocol types, weaknesses and enhancements, WPA protocol types, WPA improvements such as cryptographic message integrity code or MIC, new IV sequencing discipline, per packet key mixing function and rekeying mechanism. They also explained major problems on WPA that happened on PSK part of algorithm. Finally paper explained third generation of wireless security protocol as WPA2/802.11i.

The KirtiRaj Bhatele, et al., (2012) presented hybrid security protocol for better security using a combination of both symmetric and asymmetric cryptographic algorithms. In this hash value of the decrypted message using AES algorithm is calculated using MD5 algorithm. This hash value has been encrypted with dual RSA and the encrypted message of this hash value also sent to destination. Now at the receiving end, hash value of decrypted plaintext is calculated with MD5 and then it is compared with the hash value of original plaintext which is calculated at the sending end for its integrity. By this we are able to know whether the original text being altered or not during transmission in the communication medium.

## SECURITY CHALLENGES

Since Wireless Ad-hoc Networks are inherently different from the well-known wired networks, it is an absolutely new architecture. Thus some challenges raise from the two key aspects: self-organization and wireless transport of information, .

First of all, since the nodes in a Wireless Ad-hoc Network are free to move arbitrarily at any time. So the networks topology of MANET may change randomly and rapidly at unpredictable times. This makes routing difficult because the topology is constantly changing and nodes cannot be assumed to have persistent data storage. In the worst case, we do not even know whether the node will still remain next minute, because the node will leave the network at any minute.

One of the earliest researches in security in wireless MANET was presented in 2002. Some security challenges in MANET were inherited from ad hoc networks that were research interests since 1999. Generally there are two important aspects in security: Security services and Attacks. Services refer to some protecting policies in order to make a secure network, while attacks use network vulnerabilities to defeat a security service. In the next two parts, a brief discussion on these security aspects is presented.

**Security Services -**

The aim of a security service is to secure network before any attack happened and made it harder for a malicious node to breaks the security of the network. Due to special features of MANET, providing these services faced lots of challenges. For securing MANET a trade-off between these services must be provided, which means if one service guarantees without noticing other services, security system will fail. Providing a trade-off between these security services is depended on network application, but the problem is to provide services one by one in MANET and presenting a way to guarantee each service. We discuss five important security services and their challenges as follows:

**Availability:** According to this service, each authorized node must have access to all data and services in the network. Availability challenge arises due to MANET's dynamic topology and open boundary. Accessing time, which is the time needed for a node to access the network services or data is important, because time is one of the security parameters. By using lots of security and authentication levels, this service is disregarded as passing security levels needs time. Authors in provided a new way to solve this problem by using a new trust based clustering approach. In the proposed approach which is called ABTMC (Availability Based Trust Model of Clusters), by using availability based trust model, hostile nodes are identified quickly and should be isolated from the network in a period of time, therefore availability of MANET will be guaranteed.

**Authentication:** The goal of this service is to provide trustable communications between two different nodes. When a node receives packets from a source, it must be sure about identity of the source node. One way to provide this service is using certifications, whoever in absence of central control unit, key distribution and key management is challengeable. In the authors presented a new way based on trust model and clustering to public the certificate keys. In this case, the network is divided into some clusters and in this clusters public key distribution will be safe by mechanisms provided in the paper. Their simulation results show that, the presented approach is better than PGP. But it has some limitations like clustering. MANET dynamic topology and unpredictable nodes position, made clustering challengeable.

**Data confidentially:** According to this service, each node or application must have access to specified services that it has the permission to access. Most of services that are provided by data confidentially use encryption methods but in MANET as there is no central management, key distribution faced lots of challenges and in some cases impossible. Authors in proposed a new scheme for reliable data delivery to enhance the data confidentially. The basic idea is to transform a secret message into multiple shares by secret sharing schemes and then deliver the shares via multiple independent paths to the destination. Therefore, even if a small number of nodes that are used to relay the message shares, been compromised, the secret message as a whole is not compromised. Using multipath delivering causes the variation of delay in packet delivery for different packets. It also leads to out-of-order packet delivery.

**Integrity:** According to integrity security service, just authorized nodes can create, edit or delete packets. As an example, Man-In-The-Middle attack is against this service. In this attack, the attacker captures all packets and then removes or modifies them. Authors in presented a mechanism to modify the DSR routing protocol and gain to data integrity by securing the discovering phase of routing protocol.

**Non-Repudiation:** By using this service, neither source nor destination can repudiate their behaviour or data. In other words, if a node receives a packet from node 2, and sends a reply, node 2 cannot repudiate the packet that it has been sent. Authors in presented a new approach that is based on grouping and limiting hops in broadcast packets. All group members have a private key to ensure that another node couldn't create packets with its properties. But creating groups in MANET is challengeable.

**Attacks -**

Due to special features like hop-by-hop communications, wireless media, open border and easy to setup, MANET became popular for malicious nodes. Some of the most important attacks in MANET are as follows:

**Black Hole Attack:** In this attack, malicious node injects fault routing information to the network and leads packets toward itself, then discards all of them. In we present a survey on black hole detection and elimination approaches. Also we presented a classification of defeating approach for this attack.

Authors in  presented a new approach based on confirming the best path using second path. In this approach, whenever a source node receives RREP packets, it send

a confirmation packet through the second best path to the destination and ask the destination whether it has a route to the RREP generator or to the Next_Hop_Node of RREP generator or not.

If the destination has no route to this nodes, both RREP generator and it'sNext_Hop_Node will mark as malicious nodes. Using this approach source node can detect cooperative malicious nodes. Whoever in the case of more than two cooperative malicious node, this approach can't detect all malicious nodes.

**Worm Hole Attack:** In worm hole attack, malicious node records packets at one location of the network and tunnels them to another location . Fault routing information could disrupt routes in network . Authors in presented a way to secure MANET against this attack by using encryption and node location information. But as mentioned before, key distribution is a challenge in MANET.

**Byzantine attack:** In this attack, malicious node injects fault routing information to the network, in order to locate packets into a loop. One way to protect network against this attack is using authentication. Authors in presented a mechanism to defeat against this attack using RSA authentication.

**Snooping attack:** The goal of this attack is accessing to other nodes packets without permission. As in MANET packets transmitted hop by hop, any malicious node can capture others packets.

**Routing attack:** In this attack, malicious node tries to modify or delete node's routing tables. Using this attack, malicious node destroys routing information table in ordinal nodes. Therefore, packet overhead and processing time will increase.

**Resource consumption attack:** In this attack, malicious node uses some ways to waste nodes or network resources. For instance, malicious node leads packets to a loop that consists of ordinal nodes. As a result, node's energy consumed for transmitting fault packets. In addition, congestion and packet lost probability will increase.

**Session hijacking:** Session hijacking is a critical error and gives an opportunity to the malicious node to behave as a legitimate system. Using this attack, malicious node reacts instead of true node in communications. Cryptography is one of the most efficient ways to defeat this attack.

**Denial of service:** In this attack, malicious node prevents other authorized nodes to access network data or services. Using this attack, a specific node or service will be inaccessible and network resources like bandwidth will be wasted. In addition, packet delay and congestion increases.

## SECURITY SOLUTIONS

We have observed several vulnerabilities that capability makes the mobile ad hoc networks unsure in this paper. However, it is achieved greatest goal to secure the mobile ad hoc network if we merely know the existing vulnerabilities in it. As a result, we need to obtain some security solutions to the mobile ad hoc network. In this paper, we survey some security schemes that can be useful to protect the mobile ad hoc network from spiteful behaviors.

### A. Security Criteria

Previous we discuss the solutions that can help sure and safe the mobile ad hoc network, we think it is mandatory to find out how we can judge if a mobile ad hoc network is safe or not, or in other words, what should be covered in the security criteria for the mobile ad hoc network when we want to inspect the security state of the mobile ad hoc network. In the given sections, we briefly discuss the widely-used criteria to calculate if the mobile ad hoc network is confident.

1. Availability - The term Availability means that a node should maintain its ability to provide all the designed services regardless of the security state of it . This security criterion is faced mainly during the rejection-of-service attacks, in which all the nodes in the network cannot be available the attack target and thus some greedy nodes make some of the network services, such as the routing protocol or other key management service .

2. Integrity - Integrity defines the identity of the messages when they are forwarded. Integrity can be compromised mainly in two ways :

**Spiteful altering**

**Accidental altering**

A message can be removed, resume or revised by an competitor with spiteful goal, which is regarded as spiteful altering; on the contradictory, if the message is discard or its content is changed due to some benign failures, which may be sending errors in communication or hardware errors such as hard disk failure, then it is categorized as accidental altering.

3. Confidentiality - Confidentiality define the certain information is only accessible by authorized users. In other words, in order to maintain the confidentiality of some confidential information, we need to keep them privacy from all entities that do not have the freedom to access them.

4. Authenticity - Authenticity is essentially assurance that participants in communication are genuine and not impersonators . It is necessary for the communication participants to prove their identities as what they have claimed using some techniques so as to ensure the authenticity. If there is no confirmed mechanism, the competitor could masquerade a liberal node and thus get access to confidential sources, or even generate some fake messages to disturb the network operations.

5. Authorization - Authorization define an entity is issued a license, which specifies the advantage and permissions it has and cannot be prevented, by the licenses authority. Authorization is generally used to assign different access gadget to different level of users. For instance, we need to confirm that network management function is only accessible by the network management. Therefore there should be an authorization process before the network management accesses the network management functions.

**B. Attack Types in Wireless Mobile Ad Hoc Networks**

There are several kinds of attacks in the mobile ad hoc network, there are classified the following two types :

(i). External attacks, in which the attacker target to reason of congestion, generate entrusted routing information or disturb nodes from providing services.

(ii). Internal attacks, in which the competitor wants to collect the normal access to the network and attempt the network activities, either by some spiteful imitation to get the access to the network as a new node, or easily compromising with current node and using it as a basis to conduct its spiteful behaviors.

1. Denial of Service (DoS) - The first attack is denial of service, which aims to sure the availability of certain node or even the services of the entire ad hoc networks. In the conventional wired network, the DoS attacks are taken out by some kind of network traffic to the target so as to disable the processing power of the target and make the services provided by the target become unavailable. The mobile ad hoc networks are more vulnerable than the wired networks because of the

Interference-prone radio channel and the limited battery power. During practice, the attackers Often use the radio jamming and battery consumption methods to conduct DoS attacks to the mobile ad hoc networks, which well correspond to the two vulnerabilities.

2. Impersonation - Impersonation attack is a severe threat to the security of mobile ad hoc network . As we can see, if there is not such a proper authentication mechanism among the nodes, the contestant can take some nodes in the network and make them look like benign nodes. In this field, the adjusted nodes can join the network as the normal nodes and begin to conduct the spiteful behaviors such as propagate fake routing information and gain inappropriate priority to access some confidential information.

3. Eavesdropping - Eavesdropping is another type of attack that usually occurs in the mobile ad hoc networks. The aim of eavesdropping is to achieve some confidential information that should be kept secret during the conversation. The confidential information may include the area, public key, private key or even passwords of the nodes. Because these data's are very important to the security field of the nodes, they must be kept away from the illegal access.

4. Attacks against Routing - Routing is one of the most important services in the network; therefore it is also one of the main targets to which attackers conduct their spiteful nature. In the mobile ad hoc networks, attacks against routing are simply classified into two categories: attacks on routing protocols and attacks on packet forwarding/delivery. Attacks on routing protocols aim to block the motion of the routing information to the victim even if there are some routes from the victim to other targets. Attacks on packet forwarding try to interrupt the packet delivery along a predefined path.

The first main effects brought by the attacks against routing protocols include network division, routing loop, resource removal and route hijack. The second category of attacks against routing is attacks on packet forwarding/delivery, which are not easy to detect and prevented. There are two main attack strategies in this type: one is selfishness, in which the spiteful node selectively drops route messages that are assumed to forward in order to save it own battery power; the other is dismissal-of-service, in which the competitor sends out overwhelming network traffic to the victim to emit its battery power.

**C. Secure Routing Techniques in Wireless Mobile Ad Hoc Network**

There are different kinds of attacks against the routing layer in the mobile ad hoc networks, some of which are more discreetly and harder to detect than others, such as two attack like that Wormhole attacks and Rush attacks.

1. Defense Method against Wormhole Attacks in Mobile Ad Hoc Networks Wormhole attack is a threatening attack again routing protocols for the mobile ad hoc networks. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to different location, and resume them there into the network. The resume of the information will make biggest confusion to the routing issue in mobile ad hoc network because the nodes that get the resumed packets cannot differ it from the real routing packets.

2. Defense Mechanism against Rushing Attacks in Mobile Ad Hoc Networks Rushing attack is a new attack that results in denial-of service when used against all previous on-demand ad hoc network routing protocols. This attack is also particularly damaging because it can be performed by a relatively weak attacker.

## RESEARCH METHODOLOGY

The main goal of Wireless Ad-hoc network is to establish trusted connection amongst each other. In detection based approaches, Unified trust management security scheme is one of the important methods. By using trust information, node does not take highly risky action such as forwarding or sending the data packet to the node which is having low trust value. In trust management security scheme, trust model has two components: trust value which is calculated from direct observation & indirect observation. In direct observation, trust value is calculated from an observer node to observed node. Indirect observation is also referred as secondhand information which is obtained from neighbor nodes of the observer node. Indirect observation or second-hand information is used to evaluate trust value of observed nodes from neighbor node. Indirect information is very important as Compared to direct observation.

The main goal to adopt research methodology is to produce new knowledge, and here is the form of research methods:

Constructive research - It develops solutions to a problem. Here we will divide our work into two models theoretical model and simulation model. In the theoretical model we will study different security issues and their solutions. In the simulation model we will run simulation with MANET configuration and try to learn mechanisms which will help us to enforce security in Wireless Ad-hoc Networks.

## RESEARCH GOALS

In this paper we mainly focus on the security threats and challenges in Wireless Ad-hoc Networks. There are two main parts of our paper, in the first goal we will discuss different security aspects and how these issues to be resolved? In the second goal of the paper there is an implementation of Wireless Ad-hoc Networks in OPNET simulator; first we will develop Wireless Ad-hoc Networks network with different routing protocols and compare results with respect to throughput, bandwidth, delay etc in order to develop a better understanding of routing protocols with respect to different network situations. Second we will develop a MANET network with an intruder and discuss an integrity aspect in the network. Finally we will develop a scenario about information security. The solutions of the problem are also discussed in the document; our paper also provides good understanding of the security challenges and solutions of the Wireless Ad-hoc Networks.

## CONCLUSION

For the design of routing protocols for wireless ad hoc networks, the characteristics of the wireless channel cannot be ignored. Most current routing protocols are derived from wired versions and may perform sub optimally, in particular in mobile scenarios where fading needs to be considered.

This problem is also reflected in the models that are frequently used for the analysis and design of protocols, since these models do not capture essential properties of the wireless channel such as interference, fading, and noise.

Mobile ad-hoc networks have properties that increase their vulnerability to attacks. Unreliable wireless links are vulnerable to jamming and by their inherent broadcast nature facilitate eavesdropping. Constraints in bandwidth, computing power, and battery power in mobile devices can lead to application specific trade-offs between security and resource consumption of the device. Mobility/Dynamics make it hard to detect behavior anomalies such as advertising bogus routes, because routes in this environment change frequently. Self-organization is a key property of ad-hoc networks. Besides authentication, confidentiality, integrity, availability, access control, and non-repudiation being harder to enforce because of the properties of mobile ad-hoc networks, there are also additional requirements such as location confidentiality,

cooperation fairness and the absence of traffic diversion.

## REFERENCES


- A.Gantes and j. stucky, "A platform on a Mobile Ad hoc Network challenging collaborative gaming," international symposium on collaborative technologies and systems, 2008.
- A.Gin and R. Hunt, Editors, “Performance Analysis of Evolving Wireless IEEE 802.11 Security Architectures”, ACM International Conference on Mobile Technology Applications and Systems, (2008).
- A.H. Lashkari and M. M. S. Danesh, Editors, “A Survey on Wireless Security Protocols WEP, WPA and WPA2/802.11i”, IEEE International Conference on Computer Science and Information Technology, (2009) August 8-11, Beijing.
- B.Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour. A survey of routing attacks in mobile ad hoc networks. Security in wireless mobile ad hoc and sensor networks, October 2007, page, 85-91
- E.M. Belding-Royer and C.-K. Toh. A review of current routing protocols for ad-hoc mobile wireless networks. IEEE Personal Communications Magazine, pages 46–55, April 1999.
- F.S.a and R. Anderson, "The Resurrecting Ducking: Security Issues for Ad-Hoc Wireless Networks," 7th Int’l. Wksp on Security Protocols. Proc., LNC, 1999.
- G.Selim, H. M. E. Badawy and M. A. Salam, Editors, “New Protocol design for Wireless Networks security”, IEEE International Conference on Computer Science and Information Technology (ICACT), (2006) Feb 20-22.
- K.Bhatele, A. Sinhal and M. Pathak, Editors, “A Novel Approach to the Design of New Hybrid Security Protocol Architecture”, IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), (2012) August 23-25, Ramanathapuram.
- M.G. Zapata and N. Asokan, “Securing Ad-Hoc Routing Protocols,” Proc. 2002 ACM Wksp. Wireless Sec., Sept. 2002, pp. 1–10.
- R.Sheikh, M. S. Chande, and D. K. Mishra, "Security issues in MANET:A review," presented at the Seventh International Conference On Wireless And Optical Communications Networks (WOCN), 2010.
- S.a.A.k.G, H.o.d.R.m, and S. sharma, "A Comprehensive Review of Security Issues in Manets," International Journal of Computer Applications vol. 69 2013.
- S.Michell and K. Srinivasan, Editors, “State Based Key Hop Protocol: A Lightweight Security Protocol for Wireless Networks”, ACM international workshop on performance evaluation of wireless adhoc, sensor, and ubiquitous networks, (2004).
- Sanzgiri K, Dahill B, Levine B.N and Belding-Royer E.M, “A secure routing protocol for Ad-hoc networks,” Proc. Of IEEE ICNP, 2002
- Tao Lin, “Mobile Ad-hoc Network Routing Protocols: Methodologies and Applications”, Ph.D. Dissertation, Computer Engineering, Virginia Polytechnic Institute and State University, Blacksburg, Virginia, 2004.
- W.Arbaugh, N. Shankar, and Y.C. Wan. Your 802.11 wireless network has no clothes. Technical report, Dept. of Computer Science, University of Maryland, March 2001.
- Y.Hu, A. Perrig and D. Johnson, Wormhole Attacks in Wireless Networks, IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, February 2006.
- Y.Zhang, W. Liu, W. Lou, and Y. Fang, “Securing mobile ad hoc networks with certificateless public keys,” IEEE Trans. Dependable and Secure Computing, vol. 3, pp. 386–399, Oct.–Dec. 2006.
- Yi-an Huang and Wenke Lee. “Attack analysis and Detection for Ad hoc Routing protocols”. Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID'04), French Riviera, France. September 2004.