American Journal of Networks and Communications
2015; 4(3-1): 27-34
Published online January 16, 2015 (http://www.sciencepublishinggroup.com/j/ajnc)
doi: 10.11648/j.ajnc.s.2015040301.16
ISSN: 2326-893X (Print); ISSN: 2326-8964 (Online)

Security in ad hoc networks

Sanjana Lakkadi, Amit Mishra, Manish Bhardwaj

Department of Computer science and Engineering, SRM University, NCR Campus, Modinagar, Ghaziabad, India

Email address:
sanjanalakkadi@gmail.com (S. Lakkadi), amit_mishra65@outlook.com (A. Mishra), aapkaapna13@gmail.com (M. Bhardwaj)

To cite this article:
Sanjana Lakkadi, Amit Mishra, Manish Bhardwaj. Security in Ad Hoc Networks. *American Journal of Networks and Communications*. Special Issue: Ad Hoc Networks. Vol. 4, No. 3-1, 2014, pp. 27-34. doi: 10.11648/j.ajnc.s.2015040301.16

Abstract: Ad hoc networks are a wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead, these networks are self-configurable and autonomous systems which are able to support movability and organize themselves arbitrarily. These unique characteristics of ad hoc networks pose a number of challenges for the implementation of security infrastructure in the wireless network system design. In this paper, we study the ad-hoc architecture thus understanding the vulnerabilities and security goals. Further, we discuss the various security attacks and explore approaches to secure the communication.

Keywords: ARPANET, MANET, OSPF, QOS.

1. Introduction

Internet usage has skyrocketed in the last decade, propelled by web and multimedia applications. While the predominant way to access the Internet is still cable or fiber, an increasing number of users now demand mobile, ubiquitous access whether they are at work, at home or on the move. For instance, they want to compare prices on the web while shopping at the local department store, read e-mail while riding a bus or hold a project review while at the local coffee shop or in the airport lounge. The concept of wireless, mobile Internet is not new. When the packet switching technology, the fabric of the Internet, was introduced with the ARPANET in 1969, the Department of Defense immediately understood the potential of a packet switched radio technology to interconnect mobile nodes in the battlefield. The DARPA Packet Radio project helped establish the notion of ad hoc wireless networking. This is a technology that enables untethered, wireless networking in environments where there is no wired or cellular infrastructure (example - battlefield, disaster recovery, etc.); or, if there is an infrastructure, it is not adequate or cost effective. Ad hoc networks may be different from each other, depending on the area of application: For instance, in a computer science classroom an ad hoc network could be formed between students' PDAs and the workstation of the teacher. In another scenario, a group of soldiers are operating in a hostile environment, trying to keep their presence and mission totally unknown from the viewpoint of the enemy. The soldiers carry wearable communication devices that are able to eavesdrop on the communication between enemy units, shut down hostile devices, divert the hostile traffic arbitrarily or impersonate themselves as the hostile parties. As it can be seen, these two scenarios of ad hoc networking are very different from each other in many ways: In the first scenario the mobile devices need to work only in a safe and friendly environment where the networking conditions are predictable. Thus no special security requirements are needed. On the other hand, in the second and rather extreme scenario the devices operate in an extremely hostile and demanding environment, in which the protection of the communication and the mere availability, access and operation of the network are both very vulnerable without strong protection [2].

The challenge lies exactly in securing the ad hoc network operation, because any malicious or selfish network entity can disrupt, degrade, or even deny communication of other entities. Securing the network operation is paramount for both civilian and tactical applications [1]. Users would have no incentive to embrace new products if, for example, they cannot access their services and get the quality they paid for due to available resources being monopolized by adversarial nodes, or if their privacy is at stake. Similarly, a General or a Police Commissioner would not endorse networking technologies that do not guarantee secure and reliable communications in a battlefield or an emergency situation.

2. Understanding Ad Hoc Network

Ad-hoc network is a collection of nodes that do not rely on a predefined infrastructure. The nodes are often mobile in which case the networks are called as mobile ad hoc networks (MANET).These networks are self-configurable and autonomous systems consisting of routers and hosts, which are able to support mobility and organize themselves arbitrarily. That means the topology of the ad-hoc network changes dynamically and unpredictably. These networks can be formed, merged together or partitioned on the fly with no central administrative server or infrastructure. Thus, it is difficult to distinguish between legal and illegal participants of the network system

The Mobile ad hoc network requires a highly flexible technology for establishing communications in situations which demand a fully decentralized network without any base stations, such as battlefields, military applications, and other emergency and disaster situations.

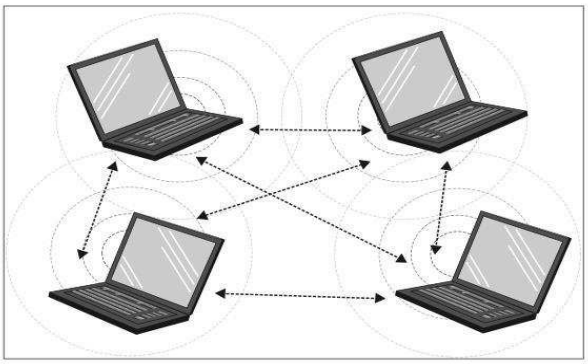

Fig 1. *Ad hoc network*

Since, all nodes are mobile; the network topology of the MANET is generally dynamic and may vary frequently. Hence, the protocol such as 802.11 to communicate via same frequency require power consumption directly proportional to the distance between hosts and direct single-hop transmissions between two hosts requires significant power that may cause interference. To avoid this problem multi-hop transmissions are used for communication. The router should be able to rank routing information sources from most trustworthy to least trustworthy and accept routing information about any particular destination from the most trustworthy sources first.

A router should provide a mechanism to filter out invalid routes and be careful while distributing routing information provided to them by another party.

Characteristics:

- Distributed Operations: Nodes' functions should be designed in a way so that they can operate efficiently under distributed conditions; supporting security and routing.
- Dynamic network topology: Connectivity of the network must be maintained to allow applications and services to operate undisrupted in a mobile scenario.
- Fluctuating link capacity: Efficient functions for link layer protection can substantially improve the link quality. Also, the bit-error rates would e high for multi-hop ad hoc networks.
- Low power devices: The nodes may be battery driven which will make the power budget tight for all power-consuming components in a device.

3. Routing Protocols in Ad Hoc

Certain unique combinations of characteristics make routing in ad hoc networks interesting. First, nodes in an ad hoc network are allowed to move in an uncontrolled manner resulting in a highly dynamic network that may cause route failures. A good routing protocol for this environment has to dynamically adapt to the changing network topology. Second, the underlying wireless channel provides much lower and more variable bandwidth than wired networks. The wireless channel working as a shared medium makes available bandwidth per node even lower. So routing protocols should be bandwidth-efficient by expending a minimal overhead for computing routes so that much of the remaining bandwidth is available for the actual data communication. Third, nodes run on batteries which have limited energy supply. In order for nodes to stay and communicate for longer periods, it is desirable that a routing protocol be energy-efficient as well. Thus, routing protocols must meet the conflicting goals of dynamic adaptation and low overhead to deliver good overall performance.

Mobile IP cannot fulfill the requirements for routing in wireless ad hoc networks in which not only the hosts but also the backbone is mobile and multi hop wireless connections composed of many links with varying quality of service (QOS) are allowed. Therefore, more adaptive network layer protocols are required. Proactive or reactive approaches can be followed when designing a routing algorithm for ad hoc networks [5].

A *proactive approach*, often also called a *table-driven approach*, is used by Internet routing algorithms like RIP, OSPF, IS–IS and BGP. In these algorithms, the routers maintain consistent, up-to-date routing information to every other node in the network. Routing tables are updated every time the topology changes. The following are examples of proactive ad hoc routing protocols [8]:

- Destination-sequenced distance vector routing;
- cluster head gateway switch routing;
- Wireless routing.

In *reactive* techniques, also called *on-demand* techniques, topology maintenance, i.e. maintaining up-to-date topology information in every router, is not continuous but is an on-demand effort. When a new packet needs to be delivered and there is not a valid route to carry out this delivery, a new route is discovered. Examples of reactive techniques are:

- flooding;
- Ad hoc on-demand distance vector routing (AODV);
- Dynamic source routing (DSR);
- Temporarily ordered routing;
- Associativity-based routing;

- signal stability routing.

A route may be unnecessarily updated many times before it is used in a proactive approach. On the other hand, the cost of route discovery every time a route is needed may be higher than the cost of maintaining an always up-to-date, consistent view of the network. This depends on the traffic generation and topology change rates. For contemporary wireless ad hoc network applications, reactive techniques such as AODV and DSR are preferred. Let us look at a few protocols in detail:

3.1. Flooding and Gossiping

In *flooding*, each node receiving a packet repeats it by broadcasting unless a maximum number of hops for the packet is reached or the destination of the packet is the node itself. Flooding is a reactive technique and it does not require costly topology maintenance or complex route discovery algorithms. However, it has several deficiencies such as:

- *Implosion* – a situation where duplicated messages are sent to the same node. For example, if node A has *n* neighbors that are also the neighbors of node B, then node B receives *n* copies of the same packet sent by node A.
- The flooding protocol does not take into account the available resources at the nodes or links, i.e. *resource blindness*.

A derivation of flooding is *gossiping*, where nodes do not broadcast but send the incoming packets to a randomly selected neighbor. Once the neighbor node receives the data, it selects another node randomly. Although this approach avoids the implosion problem by just having one copy of a packet at any node, it takes a long time to propagate the message to all nodes.

3.2. Ad Hoc On-Demand Distance Vector Routing (AODV)

AODV is an on-demand ad hoc routing scheme that adapts the distance vector algorithm to run on a network with a mobile backbone. In AODV, every node maintains a routing table where there can be at most one entry for a destination. Each entry has fields like the neighbor node to relay an incoming packet destined to a specific node and the cost of the selected route. AODV differs from the distance vector algorithm by its routing table maintenance mechanism. When a node receives a packet, it first checks its routing table to determine the next hop router for the destination in the packet. If there is an entry for the destination, the packet is forwarded to the next hop router. Otherwise a new route is discovered by broadcasting a route request (RREQ) packet.

A RREQ packet includes the following fields: source address, request id, destination address, source sequence number, destination sequence number and hop count. The source address is the address of the initiator of the route request.

If a node receives a route request that has the same source address and request id fields as those in one of the previous route request packets, it discards the packet. Otherwise it checks if there is an entry in its routing table for the destination address. If there is, the destination sequence number in the table is compared to the destination sequence number in the route request. If a router has a route for a destination in its routing table, and if it cannot reach the destination through that route, it increments the destination sequence number and sends a route request. Therefore, the destination sequence number indicates the freshness of a route. If a router has an entry for the destination in its table, and the sequence number for the request is smaller than the sequence number for the destination in its table, this means the route known by the router is fresher than the one known by the router that sends the request. In this case the receiver sends a route reply (RREP). The RREP is forwarded back to the source node through the route where the request is received. Again, this routing scheme introduces new security challenges. A malicious node may send RREP messages for every RREQ and make the other nodes forward their packets towards it. It may then sink the incoming packets, forward them to another adversary or gain unauthorized access to their contents.

3.3. Dynamic Source Routing

Another self-forming and self-healing routing protocol for ad hoc networks is dynamic source routing (DSR). It is similar to AODV in that the DSR protocol is also based on 'route discovery' and 'route maintenance' mechanisms and it is a reactive technique. On the other hand, DSR applies source routing instead of relying on the routing tables maintained by the routers. In DSR when a node has a packet and it does not know the route for the destination, it sends out a 'route request' packet. While this packet is being transferred through the network, all the nodes traversed are recorded in the packet header. A node that knows the route to the destination does not forward the packet further, but appends the route to the route information already accumulated in the packet and returns a 'route reply' packet to the source node.

After this, the source node maintains the discovered route in its 'route cache' and delivers the packets to the destination node through the discovered route by using source routing, i.e. the address of each router to visit until reaching the destination is written in the packet header by the source node. If the routing through a previously discovered route fails, a 'route error' message generated by the node that discovers the route failure is sent back to the source node, the failed route is removed from the 'route caches' and a new route discovery procedure is initiated for the destination. DSR also introduces security challenges similar to those in AODV. On the other hand, the source node controls the nodes to be traversed and this can be advantageous for security because unreliable nodes can be avoided by the source node.

4. Security Challenges

Physical security of the network elements forms the basis

for the security architecture. Further, proper key management is crucial for security in networking. The following are the areas are in question:

- Trust models
- Cryptosystems
- Key creation
- Key storage
- Key distribution

Wireless networks are susceptible to several attacks from passive eavesdropping to active impersonation, message replay and message distortion. Active attacks could range from deleting messages to injecting erroneous messages, etc. We need to consider attacks from not only the outside but from within the network as well as these nodes may be in hostile environments with low physical protection.

The following are vulnerabilities due to which security can be breached:

- Vulnerability of channels: In wireless network, messages can be eavesdropped and fake messages can be injected into the network without difficulty of having physical access to network components.
- Absence of Infrastructure: Since ad hoc networks don't work on fixed infrastructure, the classical security solutions based on certification authorities and on-line servers inapplicable.
- Vulnerability of nodes: As nodes do not reside in physically protected places they can be easily captured and fall under the control of the attacker.
- Dynamically changing topology: It is difficult to distinguish whether routing information change is due to topology change or incorrect routing information has been generated by a compromised node.

For high survivability ad hoc networks should have distributed architecture with no central entities as centrality increases vulnerabilities. Dynamic security mechanisms are needed and they should be scalable.

5. Security Goals

- *Availability*: Ensures survivability despite Denial of Service (DOS) attacks. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers, the attacker could bring down high level services e.g.: key management service.
- *Confidentiality*: Ensures certain information is never disclosed to unauthorized entities.
- *Integrity*: Message being transmitted is never corrupted.
- *Authentication*: Enables a node to ensure the identity of the peer node it is communicating with. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.
- *Non-repudiation*: Ensures that the origin of a message cannot deny having sent the message.
- *Non-impersonation*: No one else can pretend to be another authorized member to learn any useful information.
- *Attacks using fabrication*: Generation of false routing messages is termed as fabrication messages. Such attacks are difficult to detect.

6. Security Attacks

There are various types of attacks on ad hoc network which are describing following [10]:

- *Location Disclosure*: Location disclosure is an attack that targets the privacy requirements of an ad hoc network. Through the use of traffic analysis techniques [11], or with simpler probing and monitoring approaches, an attacker is able to discover the location of a node, or even the structure of the entire network.
- *Black Hole*: In a black hole attack a malicious node injects false route replies to the route requests it receives, advertising itself as having the shortest path to a destination [12]. These fake replies can be fabricated to divert network traffic through the malicious node for eavesdropping, or simply to attract all traffic to it in order to perform a denial of service attack by dropping the received packets.
- *Replay*: An attacker that performs a replay attack injects into the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions.
- *Wormhole*: The wormhole attack is one of the most powerful presented here since it involves the cooperation between two malicious nodes that participate in the network [13]. One attacker, e.g. node A, captures routing traffic at one point of the network and tunnels them to another point in the network, to node B, for example, that shares a private communication link with A. Node B then selectively injects tunneled traffic back into the network. The connectivity of the nodes that have established routes over the wormhole link is completely under the control of the two colluding attackers. The solution to the wormhole attack is *packet leashes*.
- *Blackmail*: This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender [14]. An attacker may fabricate such reporting messages and try to isolate legitimate nodes from the network. The security property of non-repudiation can prove to be useful in such cases since it binds a node to the messages it generated.
- *Denial of Service*: Denial of service attacks aim at the complete disruption of the routing function and therefore the entire operation of the ad hoc network [15]. Specific instances of denial of service attacks include the *routing table overflow and* the *sleep deprivation torture.* In a routing table overflow attack the malicious

node floods the network with bogus route creation packets in order to consume the resources of the participating nodes and disrupt the establishment of legitimate routes. The sleep deprivation torture attack aims at the consumption of batteries of a specific node by constantly keeping it engaged in routing decisions.

- *Routing Table Poisoning*: Routing protocols maintain tables that hold information regarding routes of the network. In poisoning attacks the malicious nodes generate and send fabricated signaling traffic, or modify legitimate messages from other nodes, in order to create false entries in the tables of the participating nodes [15]. For example, an attacker can send routing updates that do not correspond to actual changes in the topology of the ad hoc network. Routing table poisoning attacks can result in the selection of non-optimal routes, the creation of routing loops, bottlenecks, and even portioning certain parts of the network.
- *Rushing Attack*: Rushing attack is that results in denial-of-service when used against all previous on-demand ad hoc network routing protocols [16]. For example, DSR, AODV, and secure protocols based on them, such as Ariadne, ARAN, and SAODV, are unable to discover routes longer than two hops when subject to this attack. develop *Rushing Attack Prevention (RAP)*, a generic defense against the rushing attack for on-demand protocols that can be applied to any existing on-demand routing protocol to allow that protocol to resist the rushing attack.
- *Breaking the neighbor relationship*: An intelligent filter is placed by an intruder on a communication link between two ISs(Information system) could modify or change information in the routing updates or even intercept traffic belonging to any data session.
- *Masquerading*: During the neighbor acquisition process, an outside intruder could masquerade an nonexistent or existing IS by attaching itself to communication link and illegally joining in the routing protocol domain by compromising authentication system The threat of masquerading is almost the same as that of a compromised IS.
- *Passive Listening and traffic analysis*: The intruder could passively gather exposed routing information. Such an attack cannot effect the operation of routing protocol, but it is a breach of user trust to routing the protocol. Thus, sensitive routing information should be protected.
- However, the confidentiality of user data is not the responsibility of routing protocol.

7. Exploring the Solutions

Attack *prevention* measures, such as authentication and encryption, can be used as the first line of defense to reduce the possibilities of attacks. Most of the security research efforts in MANET to date, e.g., [33] [27] [29] [30] [31] [32] [28], are on attack prevention techniques. For example, (session) shared secret key schemes can be used to encrypt messages to ensure the confidentiality, and to some degree the authenticity (group membership), of routing information and data packets; more elaborate public key schemes can be employed to sign and encrypt messages to ensure the authenticity (of individual nodes), confidentiality, and non-repudiation of the communications between mobile nodes. The prevention schemes proposed so far differ in several ways, depending on their assumptions on the intended MANET applications.

7.1. Key and Trust Management: Preventing External Attacks [1]

Encryption, authentication, and key management are widely used to prevent external (outsider) attacks. They however face many challenges in ad-hoc networks. First, we must deal with the dynamic topologies, both in communications and in trust relationship; the assessment of whether to trust a wireless node may change over time. Second, we must deal with the lack of infrastructure support in MANET; any centralized scheme may face difficulties in deployment.

Key management consists of various services, of which each is vital for the security of the networking systems. The services must provide solutions to be able to answer the following questions:

Trust model: It must be determined how much different elements in the network can trust each other. The environment and area of application of the network greatly affects the required trust model. Consequently, the trust relationships between network elements affects the way the key management system is constructed in network.

Cryptosystems: Available for the key management: in some cases only public- or symmetric key mechanisms can be applied, while in other contexts *Elliptic Curve Cryptosystems* (*ECC*) are available. While public-key cryptography offers more convenience (e.g. by well-known digital signature schemes), public-key cryptosystems are significantly slower than their secret-key counterparts when similar level of security is needed. On the contrary, secret-key systems offer less functionality and suffer more from problems in e.g. key distribution. ECC cryptosystems are a newer field of cryptography in terms of implementations, but they are already in use widely, for instance in smart card systems.

Key creation: it must be determined which parties are allowed to generate keys to themselves or other parties and what kind of keys.

Key storage: In ad-hoc networks there may not be a centralized storage for keys. Neither there may be replicated storage available for fault tolerance. In ad-hoc networks any network element may have to store its own key and possibly keys of other elements as well. Moreover, in some proposals such as in [25], *shared secrets* are applied to distribute the parts of keys to several nodes. In such systems the compromising of a single node does not yet compromise the secret keys.

Key distribution: The key management service must ensure that the generated keys are securely distributed to their owners. Any key that must be kept secret has to be distributed so that confidentiality, authenticity and integrity are not violated. For instance whenever symmetric keys are applied, both or all of the parties involved must receive the key securely. In public-key cryptography the key distribution mechanism must guarantee that private keys are delivered only to authorized parties. The distribution of public keys need not preserve confidentiality, but the integrity and authenticity of the keys must still be ensured.

7.2. Secure Routing Protocols: Preventing Internal Attacks

To create a secure route to transport data, a proper routing protocol in Ad-Hoc networks must create a route accurately and maintain it. It means that it doesn't let the hostile nodes prevent accurate building and maintaining of the route. In general, if, in a protocol, the points such as routing signals don't counterfeit, the manipulated signals can't be injected into the network, routing messages don't change during transporting except protocol routines, routing loops don't create during aggressive activities, the shortest routes don't change by hostile nodes and so on are considered, it can be called a secure protocol [17]. To observe these points, we begin to review several protocols as far as possible.

7.3. DSR (Dynamic Source Routing)

In this protocol, the source node produces a package called RREQ in which it is determined source and target node. It sends these packages through flooding [34]. By receiving a RREQ package of each node, if it doesn't know about target route, then, it add its name to the package list and broadcast it. So, as the package reach to the target, a package includes data of route nodes and its arrangements will be available for the target node. The target node creates RREP and returns it back via available list in RREQ package header. The middle nodes know the target and do it according to the available list. So, the package traverses the route inversely to reach the source node. Although, it is a good method and certainly applicable but increases the network load and uses high band width which resulted in transporting large headers in the network. Increasing rate of header volumes resulted in increasing distance between links this approach may not work properly. OLSR works in a totally distributed manner, e.g. the MPR approach does not require the use of centralized resources. The OLSR protocol specification does not include any actual suggestions for the preferred security architecture to be applied with the protocol. The protocol is, however, adaptable to protocols such as the *Internet MANET Encapsulation Protocol* (*IMEP*), as it has been designed to work totally independently of other protocols. source and target nodes. This volume increase is due to the name of network middle elements name in the package header. Then, data sender can put the target route in the sent data header to inform middle nodes through this route that to whom they send the package. When a node can't deliver data package to the next one, it produces a package called RERR (Route Error) and returns it back to the route. So, RERR receiving nodes acknowledges about these two nodes disconnection and routing operation will be started again

7.4. AODV (Advanced On-demand Distance Vector)

In contrast to DSR protocol, this protocol doesn't put the route in the package header. But, each node controls it while receiving PREQ according to tables it had before. If the route has the final node it its table, RREP will be sent. Otherwise, it broadcasts RREQ message. Certainly, RREPs can be returned back to RREQ. It is used consecutive number in RREQ messages that a middle node gets inform whether the route is a new one. So, if the number of RREQ consecutive is smaller than route consecutive number, RREP message will be sent bymiddle node.

7.5. SAODV (Secure AODV)

As it is clear from its name, it is provided to create more security in AODV [22]. In this protocol, it is used Hash functions as it is shown in equation (1)

$$h_{n-1} = H(h_n) \quad (1)$$

In equation (1), H is the function of Hash and h is the related to the hop. In this protocol, it is used hop count to measure the number of hops in which the packages go through. If the hop count becomes more than the amount of Max Count, the package will be ignored. To prevent the changes of hop count amount and make sure about the accuracy of its amount, it is used the noted Hash functions. Due to the equation (1), each node can be sure about its authenticity by receiving a message and controlling equation (1) on it. Number n also indicates the maximum hop that a package can go through

7.6. OLSR

Optimized Link State Routing protocol (*OLSR*) [1, 24], is a proactive and table driven protocol that applies a multi-tiered approach with *multi-point relays* (MPR). MPRs allow the network to apply scoped flooding, instead of full node-to-node flooding, with which the amount of exchanged control data can substantially be minimized. This is achieved by propagating the link state information about only the chosen MPR nodes. Since the MPR approach is most suitable for large and dense ad hoc networks, in which the traffic is random and sporadic, also the OLSR protocol as such works best in these kind of environments. The MPRs are chosen so that only nodes with one-hop symmetric (bi-directional) link to another node can provide the services. Thus in very dynamic networks where there exists constantly a substantial amount of uni-directional.

5. Conclusion

We have shown that the nature of ad hoc networks has intrinsic vulnerabilities which cannot be removed. Evidently,

various attacks that exploit these vulnerabilities have been devised and studied. New attacks will no doubt emerge in the future, especially when ad hoc networking becomes widely used. Defense against these attacks can be achieved by key management or secure routing protocols. This is an important and still largely an open research area with many open questions and opportunities for technical advances.

References

[1] Security in Ad Hoc Networks, Vesa Kärpijoki, Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory, Vesa.Karpijoki@hut.fi

[2] Secure Ad Hoc Networking, Panagiotis Papadimitratos, Virginia Polytechnic, Institute and State University, papadp@vt.edu

[3] http://itlaw.wikia.com/wiki/Ad-hoc_mode

[4] Security for Ad Hoc Networks, Hang Zhao.

[5] Data Communication & Networking, Forouzan.

[6] D. M. Blough et al. On the Symmetric Range Assignment Problem in Wireless Ad Hoc Networks. In Proceedings of IFIP Conference on Theoretical Computer Science, pages 71–82, 2002.

[7] Marina and S. R. Das. Routing Performance in the Presence of Unidirectional Links in Multihop Wireless Networks. In Proceedings of ACM MobiHoc, pages 12–23, 2002.

[8] (Haas and Liang, 1999; Royer and Toh, 1999)

[9] Securing Ad Hoc Networks, Lidong Zhou, Department of Computer Science, Zygmunt J. Haas, School of Electrical Engineering

[10] Karan Singh, R. S. Yadav, Ranvijay, International Journal of Computer Science and Security, Volume (1): Issue (1) 52

[11] A REVIEW PAPER ON AD HOC NETWORK SECURITY

[12] K. Balakrishnan, J. Deng, and P.K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks" Proc. IEEE Wireless Comm. and Networking Conf. (WCNC '05), Mar. 2005

[13] Mohammad Al-Shurman and Seong-Moo Yoo, Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks" ACMSE'04, April 2-3, 2004, Huntsville, AL, USA.

[14] Yih-Chun Hu, Adrian Perrig, and David B. Johnson., "Packet Leashes A Defense against Wormhole Attacks in Wireless Ad Hoc Networks" In Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), April 2003.

[15] Patroklos g. Argyroudis and donal o'mahony, "Secure Routing for Mobile Ad hoc Networks", IEEE Communications Surveys & Tutorials Third Quarter 2005

[16] I. Aad, J.-P. Hubaux, and E-W. Knightly, "Denial of Service Resilience in Ad Hoc Networks," Proc. MobiCom, 2004

[17] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols" WiSe 2003, September 19, 2003, San Diego, California, USA.

[18] S. Prakash, J.P. Saini, S.C. Gupta, "Methodologies and Applications of Wireless Mobile Ad-hoc Networks Routing Protocols", International Journal of Applied Information Systems, Vol. 1, No. 6, pp. 5-15, February 2012.

[19] D. Johnson, D. Maltz, Y. Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)", IETF Internet-Draft, 2011.

[20] N.S.M. Usop, A. Abdullah, "Performance Evaluation of AODV, DSDV & DSR Routing Protocol in Grid Environment", IJCSNS International Journal of Computer Science and Network Security, Vol. 9, No.7, pp.261-268, July 2009.

[21] A. Akbari, M. Soruri, A. Khosrozadeh, "A New AODV Routing Protocol in Mobile Adhoc Networks", World Applied Sciences Journal, Vol. 19, No. 4, pp. 478-485, 2012.

[22] D. Benetti, M. Merro, L.Viganò, "Model Checking Ad Hoc Network Routing Protocols: ARAN vs. endairA", IEEE 8th International Conference on Software Engineering and Formal Methods (SEFM), Pisa, pp. 191-202, Sep 2010.

[23] Smith, S. Murthy, J.J. Garcia-Luna-Aceves, "Securing Distance Vector Routing Protocols", in Internet Society Symposium on Network and Distributed System Security, the 7th International Workshop on Security Protocols, San Diego, CA, USA, pp. 85-92, Feb 1997.

[24] Y.C. Hu, D.B. Johnson, A. Perrig, "Secure efficient distance vector routing in mobile wireless ad hoc networks", in Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and

[25] Applications(WMCSA'02) , pp. 3-13, June 2002.

[26] Jacquet, P. et al. Optimized Link-State Routing Protocol (OLSR). IETF draft, 18 July 2000. [referred 25.9.2000] <http://www.ietf.org/internet-drafts/draft-ietf-manet-olsr-02.txt> [in ASCII format]

[27] Zhou, L. and Haas, Z. Securing Ad Hoc Networks. 1999. [referred 25.9.2000]<http://www.ee.cornell.edu/~haas/Publications/network99.ps > [in PostScript format]

[28] S. Basagni, K. Herrin, D. Bruschi, and E. Rosti. Secure pebblenets. In Proceedings of the 2001 ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2001), Long Beach, CA, October 2001.

[29] J. Binkley and W. Trost. Authenticated ad hoc routing at the link layer for mobile systems. Wireless Networks, 7(2): 139–145, 2001.

[30] 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.

[31] S. Jacobs and M. S. Corson. MANET authentication architecture. Internet draftdraft-jacobs-imep-auth-arch-01.txt, expired 2000, February 1999.

[32] 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.

[33] A. Perrig, R. Canetti, J.D. Tygar, and D. Song. Spins: Security protocols for sensor networks. In Proceedings of the Seventh Annual ACM International Conference on Mobile Computing and Networks (MobiCom 2001), Rome, Italy, July 2001.

[34] B. R. Smith, S. Murthy, and J.J. Garcia-Luna-Aceves. Securing distancevector routing protocols. In Proceedings of Internet Society Symposium on Network and Distributed System Security, pages 85–92, San Diego, California, February 1997

[35] M. Zapata and N. Asokan. Securing ad hoc routing protocols. In Proceedings of the ACM Workshop on Wireless Security (WiSe 2002), Atlanta, GA, September 2002.