Comprehensive Overview of Security and Privacy of Data Transfer in Wireless ad Hock Network

Faten Hamad[1], Hussam N. Fakhouri[2] & Osama Rababah[2]

[1] School of Educational Sciences, The University of Jordan, Amman, Jordan

[2] King Abdullah II School of Information Technology, The University of Jordan, Amman, Jordan

Correspondence: Hussam N. Fakhouri, King Abdullah II School of Information Technology, The University of Jordan, Amman, Jordan. E-mail: h.fakhouri@ju.edu.jo

Received: February 8, 2018 Accepted: Sep. 18, 2018 Online Published: Sep. 30, 2018

doi:10.5539/mas.v12n12p185 URL: https://doi.org/10.5539/mas.v12n12p185

Abstract

Wireless ad-hoc network is a decentralized wireless network that does not have a permanent structure. Client devices are connected to form wireless network. Each node in the network to forward data from one node to another. Based on the connectivity of the network, the node dynamically determinewhich node to forward the data main threats for a secure information exchange in ad hoc networks are the unauthorized access to private data and interference in the operation of equipment and devices in order to disrupt their activity and even disable them.A possible response to these threats is the spread of independent and decentralized networks where each device is a full participant and all share responsibility for safety and security of the network. This paper provides a comprehensive overview of possible attacks. It first explores the reason and security issues in wireless ad hoc network mainly MANET and FANET, then it analyzes various types of most common threats, attacks and unresolved problems that face these types of network. After that it presents the popular security protocols to solve attack problem.

Keyword: ad hoc network, FANET, MANET, security of ad hoc network, threats of ad hoc network, privacy in ad hoc network, self organizing network

1. Introduction

The term "mobile ad hoc networking" is to some extent a synonym forthe term "mobile packet radio networks" (Mobile Packet Radio Networking). The term first came out from the early military research in 70-80-ies as "mobile mesh-networks» (Mobile Mesh Networking). It was introduced by the magazine Economist for the military networks of the future (Tamilarasan, 2012), (Kim, Min & Kim, 2004).

Wireless communication networks are divided into centralized infrastructures and self-organizing ones (SON). The distinctive feature of self-organizing networks (SON) is its ability, in the absence of a centralized infrastructure, to exchange data between any pair of nodes in the radio coverage area of network nodes. Nodes in SON can be both end hosts and routers. The connection is organized over long distances with the help of specialized routing protocols in intermediate router nodes. This connection is called "multi-stage or multi-step" (multichip). The stage is the participation of one router node in this connection. The nodes of these networks can find each other and form a network, and in the case of failure of any node, they can compose new routes for sending messages (Usop, Abdullah, & Abidin, 2009), (Luo, Wang & Chen, 2006), (Johnson & Maltz, 1996).

Ad hoc networks are set of wireless mobile communication nodes (stations, users), which form a dynamic, autonomous network with the help of mobile infrastructure. Nodes communicate with each other without centralized access points or base stations, so each node acts both as a router and as an end user. Mobile peer-to-peer networks are peer-to-peer and self-configured networks based on router nodes that are interconnected by wireless communication channels. These networks topology varies from one time to another. Each node in such a network moves randomly and independently of the other nodes in any direction. Self-configurability is necessary to make the connectivity of nodes possible. Nodesuse a common wireless channel and access to it is provided randomly. The nodes implement the transfer of data through retransmission. Therefore, the nodes in the network are not only hosts, but also routers (Tamilarasan, 2012). The most important features of such networks are: 1) the existence of a peer-to-peer structure and decentralized management; 2) unpredictable and dynamically changing topology; 3) availability of the routing function for all nodes; 4) self-organization network through retransmission; 5) various limiting factors in the network such as the variable range of radio visibility or capacity of battery devices; 6) large data loss (Transier et. al, 2004), (Tamilarasan, 2012).

2. Self-Organized Networks

There are various types of self-organized networks, includes the Mobile Ad Hoc network (MANET); Wireless Sensor Networks (WSN); Wireless Mesh Network (WMN) and Auto-Vehicle wirelessAd Hoc network (VANET). See figure 1.

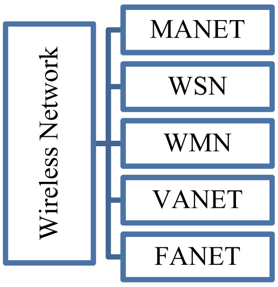

Figure 1. Wireless Network

2.1 Mobile Ad Hoc Network (MANET)

MANET is wireless decentralized self-organization network consisting of mobile devices/nodes. It consists of mobile terminals equipped with transceivers. The nodes can temporary organize network technologies for information transfer. In the MANET network, mobile devices can be either terminal stations orrouters. Each node may move in any direction and can establish connections with its neighbors. MANET needs minimal configuration for fast use of self-organization network in emergency situations such as military operations where there is no pre-deployed in-communication structure (Tamilarasan, 2012). See figure 2.

The idea of MANET came from the need to coordinate communications during combat operations in order to establish the connection between soldiers on the ground and air transport. Most communication nodes move with different speeds. Networks with fixed infrastructure cannot provide reliable communication under such conditions of high rate and high degree of unpredictability. As a rule, the MANET network does not require administration as the system administrator has little time to react and reconfigure the network. A temporary Ad Hoc network can be deployed when infrastructure creation is impossible or inefficient. MANET can be used as a temporary solution at conferences, as well as in unoccupied places where it is very difficult to create an infrastructure (Usop, Abdullah, & Abidin, 2009).

Figure 2. Mobile Ad Hoc Network (MANET)

MANET technologies are sometimes used in industrial and commercial applications, including data exchange with mobile devices. Other choices such as mobile mesh networks can be an inexpensive fault-tolerant alternative to cellular networks, i.e. military communications that need to be compatible with IP services for mobile wireless communication networks. In addition, the application of MANET technologiesis useful in developing systems of "portable" computing and communications. Well-thought-out association with satellite data transmission systems allows the creation of flexible communication systems for rescue services, firemen, etc., providing quick deployable, resilient and effective dynamic networks. Simply put, this technology provides the distribution of network IP technologies for dynamic and autonomous wireless networks (Tamilarasan, 2012).

MANET provides a fault-tolerant and efficient infrastructure by embedding routing functions in mobile nodes. It is assumed that such networks will have dynamic, sometimes rapidly changing, random multi-topology (multihop) (Fu et al., 2003). Routing support for mobile hosts is developed as part of the mobile technology IP. This technology is designed to support roaming of roaming hosts, which can connect to the internet in various ways with the ability to change the used block of addresses (Hudaib & Fakhouri, 2018). A host can connect directly to a fixed network (foreign), and/ora wireless connection. Support for these forms of mobility of hosts requires address management, enhanced protocol interoperability and support function such as hop-by-hop routing based on existing routing protocols operating in the stationary networks. In contrast, the task of specialized mobile networks (mobile ad hoc network) is the extension of mobility to the region of autonomous mobile wireless domains where a plurality of nodes and its capability of integrating the functions of hosts and routers, themselves form a network infrastructure routing (Holland & Vaidya, 2002).

One of the problems of implementing class networks MANET is to ensure efficiency, security and reliability of data transmission in the conditions of arbitrarily changing physical network topology. This problem can be solved with the help of a suitable implementation of protocol security.

Reliable delivery protocols are needed for the operation of many network applications (Gummalla & Limb, 2000). The common transport protocol is the Transmission Control Protocol (TCP) (Usop, Abdullah &Abidin, 2009). It is known that TCP is intended to provide reliable delivery of data in the traditional network, such as Ethernet, however, (Luo et al., 2006) and (Kim et al., 2004) indicated that data transmissioncontrol algorithms, presented in the TCP, are not effective in MANET networks. This is due to some reasons includes, high level of errors, conflicts and collisions on channel and physical levels, the possibility of a short-term break in communication, change of connectedness, constant change in the quality of links, application of multidirectional routing and finally the high requirement of energy for more efficiency (Toh, Cobb & Scott, 202).

Currently, there are analogue solutions for the above problem are TCP withTCP-F (Hong, 2004), TCP-ELFN (Maleki, Dantu & Pedram, 2003), and ATCP (Zhang, Lee & Huang, 2003), TCP without feedback (Chen ET. AL, 2004) and ATP (Sundaresan, 2005). The main disadvantages of the above analogues is the absence of changes in the level, the complication of the existing protocol TCP instead of its full processing. Therefore it is necessary to develop comprehensive solution problems for effective data transmission in MANET networks.

2.1.1 Characteristics of MANET Networks

The MANET network consists of mobile platforms hereinafter referred to as "nodes", which can be arbitrarily moved. Nodes can be placed on airplanes, ships, trucks and even people and every router can have many hosts. MANET is an autonomous system of mobile nodes. The system can work asisolated or have gateways or interfaces to fixed networks. In the latter case, such a network is usually is considered as a stub network connected to a fixed network. End networks transmit traffic of their nodes, but do not allow the transmission of "transit" traffic (Anupama & Sathyanarayana, 2011).

The MANET nodes are equipped with wireless transmitters and receivers that use antennas that can be omnidirectional for broadcast directed to point-to-point connections. Combinations of these antennas may also be used. At each moment, depending on the location of nodes, coverage areas of their receivers and transmitters, transmit power level and level of interaction between channels, the picture of wireless connectivity has the form of a random multi-hair (multihop) or an ad hoc network. The topology of such a network can change over time as a result of moving nodes or change their reception and transmission parameters (Barolli,Koyama, &Shiratori, 2003).

2.1.2 The Distinguishing Characteristics of MANET

As illustrated in figure 3, MANET is distinguished by four characteristics:

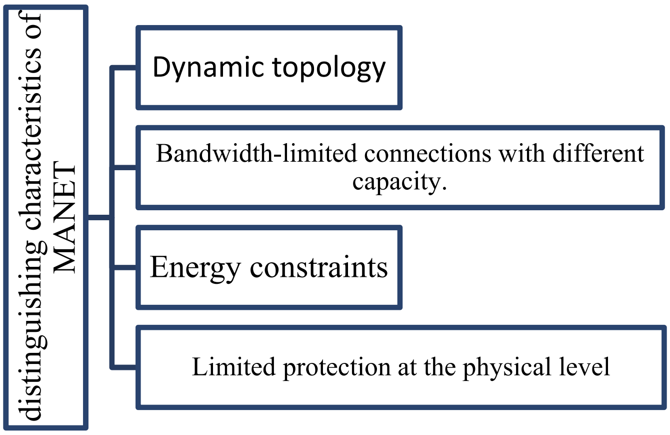
distinguishing characteristics of MANET
Dynamic topology
Bandwidth-limited connections with different capacity.
Energy constraints
Limited protection at the physical level

Figure 3. Distinguishing characteristics of MANET

1)Dynamic topology. Network nodes can be moved arbitrarily and the network topology (usually includes multiple routing intervals) can quickly change randomly at an unpredictable moments, and can also include two-way and one-way connections (Kaliaperumal& Ebenezer, 2005).

2) Bandwidth-limited connections with different capacity. Wireless Connectivity substantially loses the bandwidth of the cable lines. In addition, the throughput of wireless connections, taking into account the effect of multiple access, attenuation, noise, interference etc., is often significantly lower than the maximum speed in the radio channel. Relatively low bandwidth makes congestion in the network a rule rather than an exception. Because mobile networks are often simply an extension of the existing infrastructure, users of these networks usually want to receive the same services as fixed connection (Hussein, Salem & Yousef, 2008).

3) Energy constraints. Part or all of the MANET network nodes are being run on batteries or other sources with limited capacity. Energy saving issue plays an important role for such nodes (Leu et al., 2006).

4) Limited protection at the physical level. Mobile wireless networks are generally less protected from physical security threats, rather than cable networks. It is necessary to take into account high probability of interception and substitution of data, as well as attacks on the denial of services. Often wireless networks use different methods for protecting the channels (Fathi & Taheri, 2010).

2.1.3 MANET Network Routing Protocols

In accordance with the router strategy, the routing protocols can be divided into table-driven and on-demand routing protocols. Protocols managed by tables are also called proactive; because they collect information about the network topology before the transfer is being initialized. Each node in the network contains a routing table, which contains all the necessary information about the path to any other node on the network. This table and the information in it are updated periodically at a certain time interval or as the network topology changes. Many protocols from this category were created on the basis of classic TCP/IP network routing protocols. There are slight differences between the protocols in this category, depending on what information is contained in the routing tables. Moreover, different protocols store and update different number of tables. Proactive protocols are not suitable for large networks, since they require the availability of information about each node in the network(Barolli et. al, 2003).

On the other hand, on-demand routing protocols are called reactive protocols. These protocols do not have information about possible paths before the connection is being initialized. Routing tables are not supported in these protocols. If one node wishes to send a packet to another node, the routing reactive protocol will search for a possible path on demand and establish a connection after it finds the receiver. An important task of the reactive protocol is to maintain the established route, since the probability of disconnection is high. Compared to proactive protocols, reactive protocols have less redundancy and greater scalability. However, with the use of reactive protocols, significant delays in data transmission are possible, since the search for the desired route is done prior to data transmission. This category includes the AODV protocol (Zhong &Hanzo, 2010; Himral, Vig & Chand, 2011).

2.1.4 Requirements for Routing Protocols in MANET

Since self-organizing network does not have a fixed infrastructure, network nodes are both mobile terminals and routers. Routing in self-organizing packet radio networks is a complex task. Communication between nodes on the radio channel is often intermittent, episodic and cannot be guaranteed. Due to the mobility of nodes and the spontaneous organization of connections, the network topology undergoes frequent, unpredictable and significant changes. The range of radio communication in the network is limited and direct communication between many pairs of nodes is impossible. In this connection it is necessary to use routing with multiple transitions and jumps. With this routing, the packet is transferred from one node to another until it reaches the recipient. Routing protocols for self-organizing packet radio networks should have the following properties (Ephremides, Wieselthier & Baker, 1987):

- **Distributions.** The routing protocol should not depend on some central node, because nodes can often leave the network and join it. Due to the mobility of nodes, the network may be divided (Leu,et al ,2006).
- **Absence of loops.** The absence in the route of the loops allows avoiding excessive load of the channel, overloading the processor nodes, reducing the delivery time, and reducing the power consumption of the mobile device (Konstantopoulos, Gavalas & Pantziou, 2008).
- **Operations on request.** Reactive routing protocols that establish a route on demand can reduce the amount of transmitted overhead information and, accordingly, use network resources more efficiently (Goff et. al, 2003).
- **Support for unidirectional channels.** As a rule, routing protocols are designed to work with bi-directional connections. However, in self-organizing networks unidirectional connections can be establishedvery often for the following reasons: 1) the difference in equipment characteristics of neighboring nodes, such as transmitter power and receiver sensitivity; 2) interference - interference near node A may allow it to receive packets from node B, while node B may be in the area of more severe interference; and 3) conditions of emergency situations, when the node only works on reception(Transier et al., 2004).

2.2 WirelessSensor Networks (WSN)

The Wireless sensor network WSN is a distributed network of unattended miniature nodes that collect data about environmental parameters and transmit them to the base station by relaying from node to node using wireless communication (Holland & Vaidya, 2002).

WSN consists of small sensor nodes with integrated monitoring functions for detecting certain environmental parameters, processing and transmission of data over radio channels. They can, depend on the task, be built as mesh, ad hoc and MANET topologies; automotive networks VANET (Vehicle Ad hoc Networks) (Maleki et al., 2003), (Mishra, Singh & Kumar, 2016).

Such networks are self-organizing, since their nodes are not only terminals, but also are relay-routers, relaying packets from one node to another and also finding routes to transfer the packet over, hence these networks are capable of self-organization. Such networks can consist of tens, hundreds and even thousands of nodes. The scope of such networks is quite wide. MANET networks are useful in search and rescue operations, in military tactical operations, especially, in places of large crowds. It is possible that these networks can in many cases become an alternative to mass mobile networks (Xiao, Seah & Chua, 2000).

A network node, called a sensor, contains a sensor that senses data from the external environment (the sensor itself), a microcontroller, a memory, a radio transmitter, an autonomous power source, and sometimes actuators. It is also possible to transfer control actions from network nodes to the external environment. Sensor networks are built on the basis of the protocols IEEE 802.15.4, ZigBee and DigiMesh. Using radio communication between network nodes based on the ZigBee standard, self-organizing and self-healing networks are created. For many sensor networks, mobility is not unique feature for each node (as is the case with MANET), but only for separate group of nodes. The main requirement for the protocols of sensor networks is the low consumption of energy resources. In the sensor networks, the time of their activity directly depends on the decision of the issues of power consumption of the nodes of the network (Chlamtac, Conti & Liu, 2003). See figure 4.

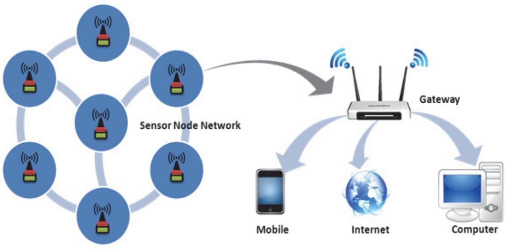

Figure 4. Wireless Sensor Networks (WSN)

There are many applications for sensor networks where different manufacturers issue different nodes for the creation of sensor networks. In the field of application, applications of sensor networks can be divided into categories such as (Luo, et al, 2006)weather, environment, agriculture;telemedicine;Emergency situations (fires, disasters, etc.);military operations, etc. (Gummalla & Limb, 2000).

2.3 Mesh Networks (WMN)

Mesh networks can be built on the basis of protocols such as 802.16 and LTE (Sarkohaki et al., 2012). The mesh network consists of a Wireless Mesh Backbone and connects the Internet, Wi-Fi networks, cellular networks, and end users. The Wireless Mesh Backbone has two types of routers; mesh-router without a gateway (Mesh Router) and Mesh-router with gateway. These routers interact with the Internet and other types of mesh-routers (Fathi & Taheri, 2010), as illustrated in figure 5.

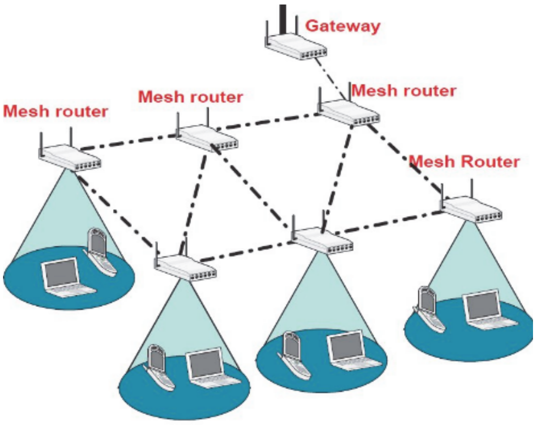

Figure 5. Mesh networks (WMN)

Mesh-router with gateway and bridge interact with all mesh-routers of the backbone network, as well as access point of WiMAX network, base stations of cellular communication network and WiMAX network, node of sensor communication network (Sink Node). Mesh-network allows subscribers to additionally provide not only internet access, but also communication among themselves within the core network. Comparing with MANET and sensor networks, cellular wireless networks differ in the following four features (Sarkohaki et Al., 2012), (Gummalla & Limb, 2000):

- Routers in mesh networks are able to pass more traffic and have fewer restrictions in terms of energy costs.
- Network marchers can provide data transfer to longer distances.
- Networks of routers can be used as an integrator of such networks as the Internet.
- Cellularnetworksand wireless local networks.

In mesh networks, any router has at least two radio channels: one for connecting clients, another for communicating with other routers. Almost any application of mobile Ad Hoc networks, discussed above, can be implemented in wireless mesh networks. The main advantage of mesh networks is its ability to transmit large amounts of data over long distances and provide broadband access (Tang, Xue & Zhang, 2005).

2.4 Vehicle Wireless Networks (VANET)

Currently, with the support of industry, government and academic institutions in the world, several research projects are being vehicleried out to develop and adopt standards for such automotive networks. The creation of automotive wireless self-organizing VANET networks is designed to improve the efficiency and safety of traffic. The main three purposes of using VANET are:1) Assistance to the driver (navigation, collision avoidance and change of lanes); 2) Informing (on speed limitation or repair area); 3) Warning (post-accident, on obstacles or condition of roads) (Kim, et al, 2004). See figure 6.

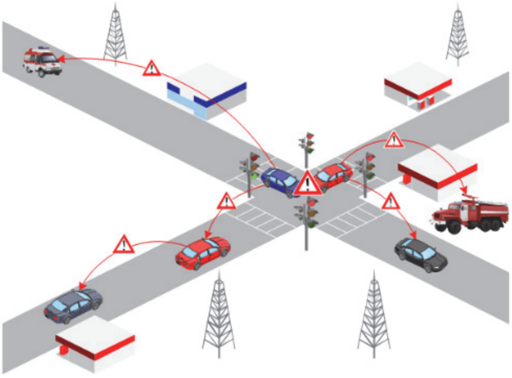

Figure 6. Vehicle Wireless Networks (VANET)

2.5 Flying Ad Hoc Network (FANET)

Flying Ad Hoc Network (FANET) similar to the MANET (Mobile Ad Hoc Network) and automotive VANET (Vehicle Ad Hoc Network) represents a special kind of peer-to-peer self-organizing network based on unmanned aerial vehicles (UAVs) (Tamilarasan, 2012). The organization of this type of communication is necessary not only to fulfill the tasks of providing surveillance, monitoring, but also, to effectively coordinate the movement of vehicles, improve as a means to prevent collisions (Leonard & Takuo, 2003) (Younis and Fahmy, 2004).

2.2 Threats to the Security of Self-Organizing Networks

There are several reasons for the vulnerability of information security of self-organizing networks includes the following (Haas & Deng, 2002):

- Vulnerability of channels to listen and substitute messages due to the overall availability of the media, as in any wireless network.
- Unprotected nodes from an attacker who can easily be removed from the network (usually located in open spaces) and use them for their own purposes.
- The lack of infrastructure makes classical security systems, such as certification centers and central servers, inapplicable.
- Dynamically changing network topology requires the use of complex routing algorithms that take into account the probability of incorrect information from compromised nodes as a result of changing the network topology.

Approaches to ensuring information security in mobile self-organizing networks significantly differ from approaches for implementing IS in wired networks due to the varying nature of the radio channel. Communication is vehicleried out through a wireless environment. Therefore, any node within the source signal range that knows the transmission frequency and other physical parameters (modulation, coding algorithm) can potentially intercept and decode the signal. And neither the source of the signal, nor the recipient will not know about it. In a wired network, on the contrary, such interception will be possible if the attacker physically has access to a wired channel, which in practice is much more complicated (Leonard & Takuo, 2003).

In centralized networks, it is easy to analyze traffic or the entire system for suspicious behavior and, if necessary, implement a specific security policy. Such a mechanism cannot be implemented in Ad Hoc, since each node in such networks has the same privileges as all the others. In addition, as mentioned above, these networks do not have a clear topology, but on the contrary, each node can move freely (Luo et al., 2006).

3. Routing Protocols for a Wireless Sensor Network

Existing MANET routing protocols cannot be used in wireless sensor networks WSN due to the following reasons:

- Restriction of energy consumption. The sensor, due to its small size, can only be equipped with a limited power source. In certain applications of sensor networks particular attention in the protocols of the march of sensor networks is given to the reduction in the frequency of information transmission / reception.
- Limited scalability. Increasing the number of sensors in the network can lead to overloading of routing tables, blocking of sensors and, accordingly, failure of the network.

Sensor Protocols for Information via Negotiation (SPIN) refers to adaptive protocols in which initially only the main characteristics of data is sent, for more economical power consumption. The complete data is transmitted only when they are requested. SPIN uses three types of messages: ADV, REQ and DATA. Before sending a message, the DATA sensor sends an ADV broadcast message containing a brief description of the complete DATA message. If a neighboring node is interested in receiving the DATA, it sends a REQ request to it in response. After receiving DATA, this neighbor node repeats the process, giving the other nodes a copy of the DATA message(Islam et al., 2016).

At the same time, it should be noted that in sensor networks, the ability to protect the network against DoS attacks routing disruptions is much less than in MANET networks. Thisis not only because of limitations of power consumption, but also due to hardware limitations (memory size of several KB, packet length of about 30 bytes). As a result, it seems almost impossible to implement mechanisms such as asymmetric cryptography, AES encryption in sensor networks. The sensor network encryption protocol (SNEP) is used to ensure data confidentiality, authentication of two data exchange participants, data integrity and repeat protection(Barolli, et al, 2003).

3.1 Rosette Protection Routing Mesh-Network

Ad Hoc networks are a set of wireless mobile communication nodes (stations, users), which form a dynamic autonomous network with the help of mobile infrastructure. Nodes communicate with each other without interference centralized access points or base stations, so each node acts both as a router and as an end user. An example is the connection of several computers wirelessly way without an access point. Often such a method of connection is used for exhibitions, in the conference halls (Tang et al., 2005), (Ni, Zhong & Zhao, 201).

On the Internet, routers within the central areas of the network own well-known operators, and therefore some degree of confidence in it. But this assumption is not valid for Ad Hoc networks because all nodes in the network participate in routing. And also as communications are usually wireless, the security of the transmission might be compromised. Moreover, due to the fact that the topology in such networks is extremely dynamic, traditional routing protocols cannot be longer used. Thus, Ad Hoc networks have much more requirements for security, sustainability and efficiency (Islam et al., 2016).

Several routing protocols have been proposed in Ad Hoc networks, and namely: AODV, DSR, ZRP, TORA, DSDV, STAR and others. But all of the above protocols have flaws and defects in the protection system, and can be easily subjected to attacks. There are two types of attacks on routing protocols in Ad Hoc networks that are; passive attacks and active attacks (Kaur, D., & Kumar, 2013).

3.2 Types of Attacks Against Routing Protocols

3.2.1 Passive Attacks

Passive attacks imply unauthorized "Eavesdropping" on packets that send routing protocols. In thisthe attacking party does not interrupt the operation of the routing protocol, but only tries to find valuable information by listening to routing traffic. Passive attacks in a wireless communication environment are usually impossible to detect. And therefore it is difficult to protect the network from such attacks. Moreover, it is possible to disclose route information about the interaction between nodes or identify their addresses. For instance, if the route to a particular network node is used more often than other nodes, this node can cause the entire network to shut down. Another "interesting" information that can be extracted from the route data is the location of the nodes. Even when it would be impossible to decide on the exact location of the site, information about network topology can be detected (Haas & Deng, 2002).

The most common problem in open and unmanaged environments, such as wireless networks isthe possibility of anonymous attacks. Anonymous attacker can intercept a radio signal and decrypt the transmitted data. The attacker must be near the transmitter in order to be able to intercept the transmission. Such interceptions are almost impossible to registerand difficult to prevent. Using antennas and amplifiers gives an attacker the opportunity to be on significant distance from the target in the interception process.Eavesdropping is conducted to collect information about the network, which subsequently is supposed to attack (Hudaib et al., 2017). The primary purpose of the attacker is to understand who is using network, what information is available, what are the capabilities of the network equipments, in what moments it is exploited the most and least and what the territory network deployment is. All this is useful in order to organize an attack on the network, for example the attacker can use the gathered information in order to gain access to network resources. Many public network protocols transmit such important information as username and password (Temel & Bekmezci, 2013). Even if the transmitted information is encrypted the attacker canregister it and then decode it. Another way to eavesdrop is to connect to a wireless network. Active eavesdropping on a local wireless network is usually based on an incorrect use the Address Resolution Protocol (ARP). Initially, this technology was created to "listen" to the network (Zhang, Lee & Huang, 2003).

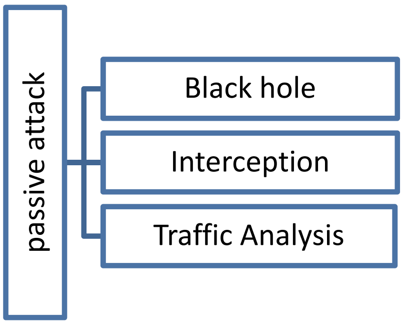

Figure 7. Passive attack

3.2.1.1 Black Hole

In this case, the hostile node uses the routing protocol for declaring itself as the shortest path to the nodes the package is intend to be sent to. In a protocol based on broadcast, such as AODV, the attacker listens to requests for routes. When an attacker receives a route request to the required node, it sends a response with an extremely short route. If the fake answer reaches the node before the correct answer, the false route is then created. It can decide to throw out package to organize a dos-attack or, conversely, as a first step, replace it for the subsequent implementation of an attack of the type "man-in-the-middle" (Chlamtac et. al, 2003).

3.2.1.2 Interception

The transmitted data can be intercepted by eavesdropping on transmission lines (radio channel). It is worth noting that wireless communication lines are easier to overhear due to the nature of the radio channel. Therefore, wireless networks are more vulnerable to passive attacks (Haas & Deng, 2002).

3.2.1.3 Traffic Analysis

Just like the content of forwarded packets, the type of the traffic can give a lot of information to the attacker. Analyzing traffic can provide important information about the network topology and routing. Based on the results of traffic analysis, an attacker can conduct an active attack and destroy a certain number of nodes, which will cause reconfiguration of the network and transfer of valuable information from the node to another. In this case information about the network topology can be collect. In active attacks, the attacker affects the operations that occur in the attacked network. Active attacks can be classified into the following groups: Physical, Falsification (spoofing), repetition and modification of messages and finallydenial of service (Kim et. al, 2004).

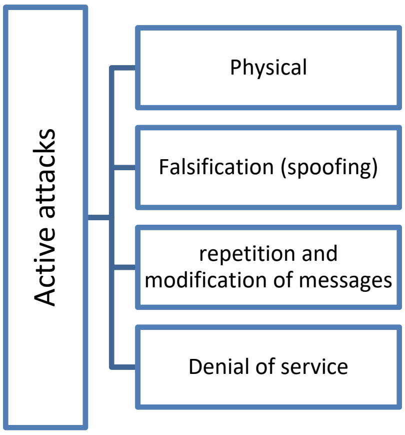

Figure 8. Active attacks

3.2.2 Active Attacks

In active attack, the attacker must be able to penetrate into an arbitrary network package. The goal may be to attract (redirect) packets destined for other nodes to the attacking side for analysis or just to disrupt the network. The main difference in comparison with passive attacks is that active attacks can sometimes be detected. Some types of active attacks are listed below as illustrated in figure 8.

3.2.2.1 Physical Attacks

An attacker can physically destroy the equipment used to destroy the node. Physical attacks aimed at equipment can be a serious problem, especially in military communications. Another type of physical attack is the electromagnetic pulse (EMR). EMR is a short-term release of electromagnetic energy, which can cause a temporary surge in voltage in all electronic devices, which can lead to their breakdown. EMP is the usual result of nuclear explosions. To date, even portable devices are available that are capable of causing EMR. Despite the fact that the use of EMP is still not always appropriate, this technology poses a threat to all electronic devices within the tactical zone (Chlamtac, et al, 2003).

3.2.2.2 Falsifying, Repeating and Modifying Messages

A falsified node behaves like another, sanctioned node. These nodes can intercept messages, save and forward them (repeat). Finally, the contents of the intercepted messages can be changed before it is delivered to the recipient.

3.2.2.3 DOS Attacks

For self-organizing networks, there are also potential threats that are realized in the form of DOS attacks aimed at violating the legitimate operation of routing. All such attacks can be divided into two types: Attack of routing violation and attack of resource consumption. The first type of attack is aimed at making the routing protocol work incorrectly and to stop performing the necessary functions. In resource consumption attacks, the goal is the consumption of network resources different as much as possible, such as channel capacity, memory, computing power and electricity (Jhaveri, Patel & Jinwala, 2012).

3.2.2.3.1 Client Station Mute

It is client jamming in order to intercept a connection. Muffling in networks occurs when a deliberate or unintended interference exceeds the capabilities of the sender or receiver in the communication channel, thus, disabling this channel (client muting). The attacker can use various methods of jamming.

Closing the client station allows the fraudster to substitute himself for the place of the muted client. Also jamming can be used for refusal in service of the client so that to it will not be possible to implement compound. More sophisticated attacks interrupt the connection to the base station to make it attached to the attacker's station (Haldar, 2009).

3.2.2.3.2 Base Station Mute

The jamming of the base station makes it possible to replace it with an attacking one. Such jamming denies users access to services.

Most wireless network technologies use unlicensed frequencies. Therefore, many devices, such as cordless phones, tracking systems and microwave ovens, can affect the operation of wireless networks and then jam the wireless connection. To prevent such cases of unintentional jamming before buying expensive wireless equipment, one must fully analyze the location of its installation. The reason is to make sure that other devices do not interfere with communications (Haldar, 2009).

3.3 Threats to Crypto Protection

In wireless networks, cryptographic is meant to ensuring the integrity and confidentiality of information. However, oversights lead to disruption of communication and malicious use information.

WEP is a cryptographic mechanism designed to provide security networks standard 802.11. This mechanism uses a single static key that is used by all users. Only the network managershave access to the keys, and hence their frequent modification and detection are impossible. However, WEP encryption is vulnerable, as the attacker can completely capture and restore the key for several hours after capturing minimum network traffic. Therefore, WEP cannot be relied upon as a means of authentication and confidentiality in wireless network (Haas & Deng, 2002), (Gagandeep & Kumar, 201).

This does not mean not to use WEP, but it means that there is a need for other methods to protect the network from attacks. All wireless communication networks are susceptible to listening attacks during the period of contact (connection setup, communication session and disconnection). The nature of wireless connection eliminates the possibility of its control, and therefore it requires protection. Also, key management, as a rule, causes additional problems when it is used while roaming in public and open environment (Song, Wong & Leung, 2004). (Hong, 2004).

3.4 Anonymity of Attacks

Wireless access provides complete anonymity of the attack. Without corresponding equipment in the network, allowing to determine the location, an attacker can easily remain anonymous and hide anywhere in the territory of the wireless network action. In this case, the attacker is difficult to catch. Figure 9 illustrates the types of anonymous attacks on wireless networks.There are several attack on ad hoc network (Jawandhiya et al., 2010), as illustrated in figure 9.

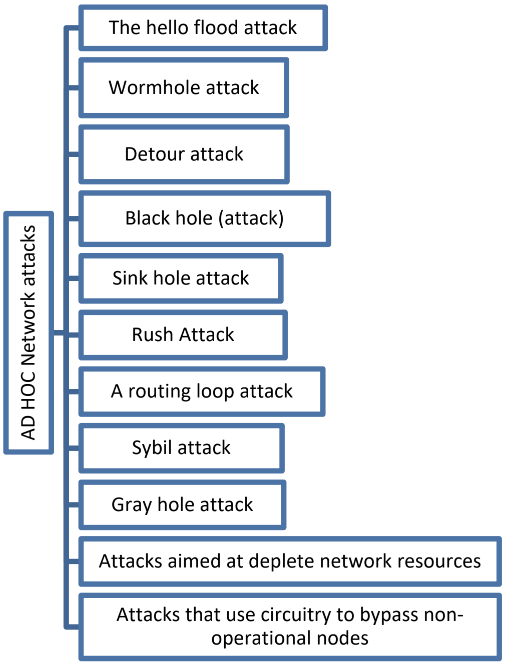

Figure 9. Ad hoc network attack

3.4.1 The Hello Flood Attack

A violating node transmits a broadcast or other information with a sufficiently powerful signal, showing each node on the network that it is their neighbor. This will cause a denial of services, means that when other nodes transmit their packets to the present neighboring nodes, their packets are not accepted by them. As illustrated in figure 10

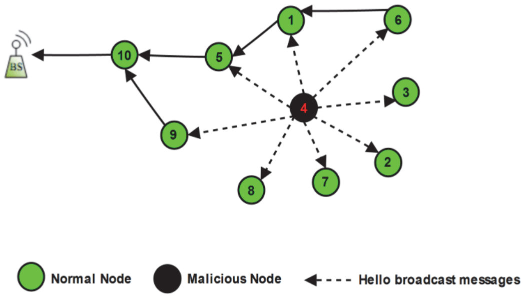

Figure 10. The hello flood attack

3.4.2 Wormhole Attack

A violating node can intercept packets at any point and forward them to another disrupting node that is located in another part of the network. This transfer will take place outside the channel band. The second node will then re-transmit the packets. All nodes that are able to hear the retransmission of the second malicious node will assume that it is the node that sent the packets and therefore it is their close neighbor. For instance, node A sends packets. These packets are then receivedby nodes B and W1. B is the authorized node while W1 is malicious. Then W1 forwards the packet to another unauthorized node W2 via a channel that is not available to other nodes of the network, except the hostile ones. W2 node then forward the packet that to reach node F. For example, packages that follow the normal path, A-B-C-D-E-F, reach node F later than those that were transmitted in the wormhole. Thus, packets that arrive with a delay will be disvehicleded due to the fact that they have more nodes traversed on the route. Wormhole attacks are very difficult to detect. They can affect the performance of many network services, such as: time synchronization, localization or data synchronization. Figure 11 illustrates the process of wormhole attacks.

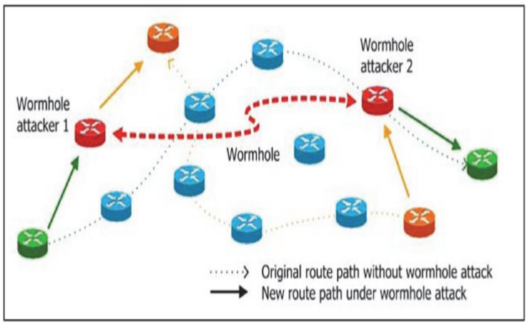
Wormhole attacker 2
Wormhole attacker 1
Wormhole
Original route path without wormhole attack
New route path under wormhole attack

Figure 11. Wormhole attack

3.4.3 Detour Attack

In this attack, an attacker can try to route traffic bypassing the main path, making the new path appear as or less than optimal rout to another part of the network. For example there is an attack such as "free bypass", where the hostile node has virtual nodes on the main path. Thus, the correct path becomes more expensive in terms of the number of hops and traffic goes around in a way that is beneficial to the attacker.

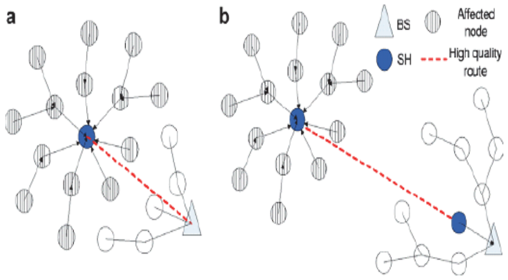

Figure 12. Detour attack

3.4.4 Black Hole Attack

A violating node can destroy all the packets that it receives for subsequent transmission. This type of attack is especially effective when the node is also a collection point. This combination might be the reason for stopping the transfer of a large amount of data. See figure 13.

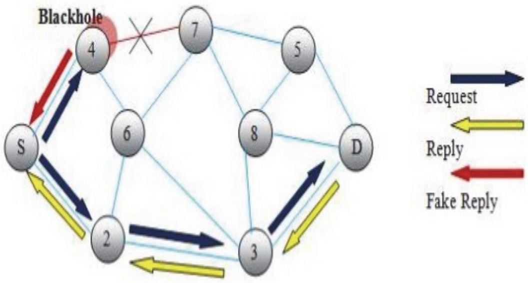

Figure 13. Black hole attack

3.4.5 Sink Hole Attack

The breaking node appeared to be the most optimal choice for all surrounding nodes from the point of view of the routing algorithm. For example, the violating node can send out routing messages, convincing all neighboring nodes that it is the best node for subsequent transmission of the packet to the base station. This allows him to become a hub and collect all the packets from all the nodes of his neighborhood going to the base station. This opens up great opportunities for subsequent types of attacks.

3.4.6Gray hole attack (selective forwarding): When the breaking node destroys all received packets, it can easily be detected by neighboring nodes. Therefore, the intruder can destroy data packets selectively, and the rest can be broadcast correctly. See figure 14.

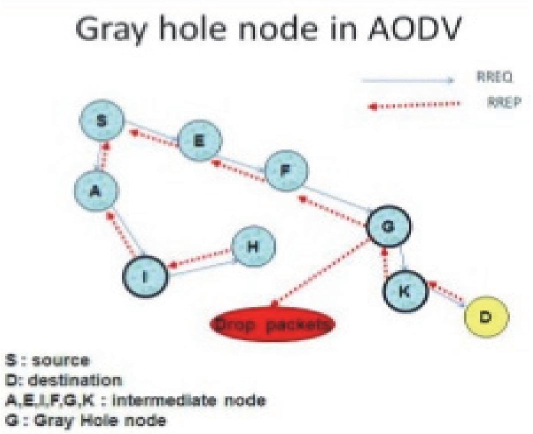

Figure 14. Gray hole attack

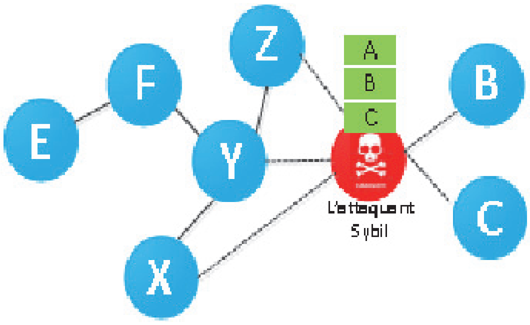

Figure 15. Sybil attack

3.4.7 Sybil Attack

One node represents several nodes for other network members. It can affect other network services, such as calculating abnormal behavior, algorithms based on voting, collecting and correlating data and distributed storage of information. This considers a big problem for routing protocols. See figure 15.

3.4.8 A Routing Loop Attack

A bypass type attack and a collection point can be used to create a loop to consume power and throughput, and also to prevent proper routing. This is illustrated in figure 16.

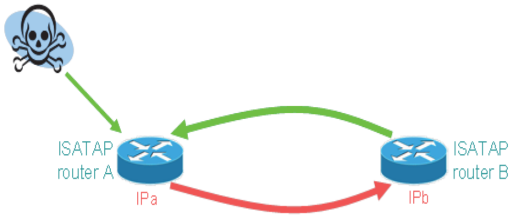

Figure 16. A routing loop attack

3.4.9 Rush Attack

The attacker disseminates the route request messages and quickly replicates these messages throughout the network. This creates congestion to other legitimate route path requests.

3.4.10 Attacks that Use Circuitry to Bypass Non-Operational Nodes

Some routing algorithms have techniques that avoid using nodes with low performance or power supplies in order to have a better chance of delivering the packet. The same schemes can be used by intruders. For example, a hostile node can send an error message to a node that actually works well. In view of this, the routing protocol will try to avoid using this node for subsequent transmission of the packet. Another example is the noise of a particular connection for a short time interval. During this interval, an error message will be generated, and the routing protocol will try to find a workaround even if this connection is no longer noisy.

3.4.11 Attacks Aimed at Depletes Network Resources

Whennodes are not constantly serviced and rely only on their limited resources, an attacker can try to deplete them to undermine the network. For sensory networks, this type of attack has great implications for the depletion of power supplies nodes. The standard method for implementing this attack is to send fictitious packets that are mandatory for processing (Mishra et al., 2016).

3.5 Physical Protection

Devices for wireless access to the network must be small, and portable (PDAs, Laptops), and access points also have small size and compactness. Theft of such devices in many respects leads to the fact, that an attacker can get into the network without using complex attacks, since the main ones authentication mechanisms in the 802.11 standard are designed to register exactly physical hardware device, not the user account. So the loss of network interface and the not timely notification of the administrator can lead to the fact that an attacker will gain access to the network without much trouble (Haas & Deng, 2002), (Xu & Gerla, 2002).

4. Basis of Cryptography

Cryptography is the science of compiling and decoding coded messages. Cryptography is an important element for authentication mechanisms, integrity and confidentiality. Authentication is a means of verifying the identity of the sender or recipient of information. Integrity means that the data has not been changed, and confidentiality creates a situation in which no one can understand the data, except their sender and recipient. Usually cryptographic mechanisms exist in the form of an algorithm (mathematical function) and a secret value (key).

4.1 Basic Terms and Their Definitions

- **Authentication**: determining the source of information, that is, the end user or device (central computer, server, switch, router, etc.) (Kumar, et al, 2006).
- **Data integrity**: ensuring the data is unchanged during transmission.

- **Data confidentiality**: ensuring that data is viewed in an acceptable format only for those who have the right to access this data.
- **Encryption**: the method of changing information in a way that it cannotbe read by anybody, except the addressee, who should decipher it.
- **Decoding**: the method of restoring the changed information and bringing it into readable form.
- **Key**: A digital code that can be used to encrypt and decrypt information, as well as for its signature.
- **Shared key**: A digital code used to encrypt / decrypt information and verification of digital signatures; this key can be widely distributed; public key is used with the corresponding private key.
- **Private Key**: a digital code used to encrypt / decrypt information and verification of digital signatures; the owner of this key must keep it a secret; the private key is used with the corresponding public key.
- **Secret key**: A digital code shared between the two parties for encryption and decryption of data.
- **Hash function**: mathematical calculation, the result of which is the sequence bits (numeric code). Having this result, it is impossible to restore the original data, used for calculation.
- **Hash**: A sequence of bits obtained by calculating a hash function.
- **Message digest**: the value produced by the hash function (the same as "hash").
- **Cipher**: any method of data encryption.
- **Digital signature:** the sequence of bits attached to the message (encrypted hash), which provides authentication and data integrity.
- **AAA (Authentication, Authorization, Accounting):** architecture of authentication, authorization and accounting.
- **VPN (Virtual Private Networks):** virtual private networks.
- **IDS (Intrusion Detection System):** intrusion detection systems.

5. Routing Protocols

This section presents a general provision on routing algorithms in self-organizing networks. Due to their high sensitivity to DoS attacks For Ad Hoc networks, it is not appropriate to use network layer routing protocols in TCP / IP networks, although they also adapt to changes in the network topology. However, in Ad Hoc networks, changes can occur very often, which can lead to frequent transmission of information about the topology change. With the growth of the network, this leads to a large expenditure of frequency, computational and energy resources. The routing protocol on the Ad Hoc network should be easily adapted to changes in the network topology when moving mobile devices (routers, terminals), optimal in terms of using network resources, is scalable. Therefore, the requirements for routing protocols are tightened in Ad Hoc. More than 30 Ad Hoc routing protocols have been developed (Haas & Deng, 2002).

5.1 Routing Table Overflow

With this attack method, the pest tries to create routes to non-existent nodes. The purpose of the attack is to create routes that would prevent the creation of new routes by overflowing the table routing protocol. The "proactive" routing algorithms are trying to learn routing information even before it is needed, while a "reactive" algorithm creates a route only if it is required for transmitting data. It turns out that this property of "preemptive" algorithms makes them vulnerable to overflow attacks on routing tables. The attacking party may just send redundant routes to the routers of the network. On the other hand, "Reactive" algorithms, such as AODV, do not collect pre-route information.

5.1.1 Testing with Insomnia

Usually, the attack is practical only in Ad Hoc networks, where the functioning devices is critically dependent on the operation of power supplies. Power Supplies try to store the stored energy by transmitting data only when it is necessary. The attacker can try to use power sources(accumulators) by using route information requests, or by forwarding unnecessary packets to other nodes, using, attacks such as a "black hole". This The attack is especially suitable against devices that do not offer any services in the network or offer services only for those who have a special permit (Sarkohaki et al., 2012).

Despite the properties of these services, the node has to participate in the process of routing if it does not want to be disconnected from the network.

5.1.2 Location Detection

Attacks of this type are trying to find out different information about the location of the nodes or the structure of the network. The information obtained could give information about which nodes are adjacent to the node of interest or the physical location of nodes. Attack can be as simple as using the equivalent of the "trace route" command on the UNIX system. Routes are sent with insufficient value of redistribution of number of hops, and addresses of devices sending ICMP error messages are recorded. In the end, the attacker knows, which nodes are located on the route to the node of interest. If the location some intermediate nodes are known, then one can also obtain information about the location of the attacked target (Mishra et. al, 2016).

5.2 Mobile IP-Based Routing

Improving mobile routing at the IP level can provide benefits similar to properties of fixed internet networks, namely, "interoperability in heterogeneous network infrastructure". In this case, the infrastructure is wireless and uses a variety of different wireless technology communications, protocols for access to channels, etc. Advanced IP routing and related network services are interlinked to ensure the integrity of mobile inter-network segments in this more dynamic environment.

In other words, the real advantage of using routing at the IP level in MANET is ensuring consistency at the network level for networks with multiple transmission intervals (multihop network), and consisting of nodes on which a "mishmash" of physical media is used (that is, a mixture of what is commonly called subnets of technology). A MANET node includes a router that can be physically connected to a multitude IP hosts (or devices with IP addresses) and potentially has a "lot" of wireless interfaces, where each of them uses its own wireless technology. Thus, the MANET node with interfaces using technology A and B, can interact with any other MANET node that has an interface with technology A or B. The multi -interconnectedness of technology A forms a multi-interval topology of the physical layer, and the multi-overlapping connectivity of technology B forms another topology of the physical layer (it may differ from the topology for A) and the union of these topologies forms a new topology (in terms of graph theory - multigraph), terminating with the "IP routing machine" of the MANET network. The MANET decision-making routing nodes using this "machine" can exchange data using either or both mentioned topologies of the physical layer. As the development of new physical layer technologies new device drivers are created, and other multi- interval data can be added to the "IP routing machine" topology of the physical layer. Some old technologies can be removed from circulation. Functional and the architectural flexibility provided by routing at the IP level will significantly reduce the hardware costs when scaling (Carollo et. al, 2008).

The concept of a node identifier (not to be confused with an interface identifier) has a decisive value to support the multigraph topology of the routing machine. This allows to unify the sets of wireless interfaces and identify them as belonging to a single mobile platform.

5.2.1 Interaction with Standard IP Routing

MANET networks are now considered stub (stub) - this means that all traffic through the MANET nodes are addressed to or originated from the MANET network. Limited capacity and possible nutritional restrictions do not allow the MANET networks to be considered as transit (although this restriction can be removed as the technology develops). This restriction substantially reduces the number of routes that are required to announce an interaction with fixed internet networks. For the terminal network, a route interaction can in the near future be provided by a combination of mechanisms such as anycast-transmissions in the scale of the MANET network and mobile IP (Tseng, Shen, & Chen, 2003).

Interaction with standard IP routing can be significantly improved by using the common MANET addressing model in all MANET routing protocols. The development of such a model will allow routing through multi-technology environments providing the ability to support multiple hosts on each router, and also guarantees long-term compatibility by architecture of IP addressing. To support these functions, there is only a need to identify host interfaces and routers to IP addresses. The identification of routers by a separate router ID and the possibility to support on a router set of wired and wireless interfaces (Hudaib, Fakhouri, 2001).

5.3 Problems with MANET Routing Protocols

To assess the merits of the routing protocol, you need a metric - both quantitative and qualitative – that will measure stability and productivity. The metric should not depend on any particular routing protocol.

5.4 Quality Indicators for the Routing Protocols MANET.

1) Distributed capabilities. Essential property that should be noted.

2) Work on requests. Instead of assuming a uniform distribution of traffic over the network (and constant support

routes to all nodes of the network), adapting the routing algorithm to change patterns of traffic by request and need. If such an adaptation is performed fairly intellectually, it allowsreducing power consumption and throughput through some increase time to find routes.

3) Proactive actions. The organization of routes on requests is associated with additional delays, which may be in some cases not acceptable. If the energy is sufficient to supply thenproactive actions for organizing routes can be used in such environments (Heenavarshney, 2013).

4) Security. Without any protection at the network and link layer, the routing protocol MANET is vulnerable to many types of attacks. It is relatively simple to organize interception of network traffic, reuse message, change package headers, and redirect route messages in wireless networks without suitable security measures. Although the mentioned problems arise in cable networks. It is desirable to provide protection that prevents violation of protocol operations. This can be implemented to some extent for any protocol routing using external tools (IP Security methods).

5) Work with "periods of sleep." In order to save energy or for other reasons, be inactive, the nodes in MANET can stop transmission and / or reception at arbitrary intervals time. The routing protocol should be adapted to such circumstances without undesirable consequences. This may require close interaction with the link layer through a standardized interface.

6) Support for one-way connections. When developing routing algorithms, it is usually assumed that there are two-way connections as many algorithms cannot work correctly through one-way connection. However, in wireless networks, one-way connections are often found. However, in situations where two parts of a specialized network are connected only by a pair one-way (with opposite directions) connections, the ability to work on a unilateral the channel becomes vital. Below is a list of quantitative parameters that can be used to assess performance any routing protocol:

1) Throughput and delay. Statistical parameters of routing performance data (mean, variation, distribution) are important. There are also characteristics of the efficiency of the route policy (how well the work is performed), estimated from "external" point of view of other rules that can use routing.

2) Time of the route. One important measurement of end-to-end delay (especially important for routing algorithms "on demand") is the time required for the organization of the route after it is being requested.

3) The proportion of packages with a violation of the order of delivery. External characteristic of routing performance without the organization of explicit connections (connectionless routing) especially interesting for protocols transport layer of the TCP type, which prefer orderly delivery.

4) Efficiency. If the efficiency of data routing is an external indicator of productivity of policy, then efficiency is an internal measure of its effectiveness. To achieve a given level of data routing performance, two different policies can spend different amounts of resources depending on their internal effectiveness. Efficiency of the protocol may have a direct or indirect effect on the performance of data routing. If a common channel with limited bandwidth is used for data and control, redundant traffic management often affects the performance of data routing. It is useful to track several coefficients that show the internal efficiency of the protocol in part of the performance of its work. Some of efficiency measurements are:

- The average ratio of transmitted / delivered data bits can serve as a measure of efficiency delivery of data on the network. Indirectly, this value also characterizes the average number of stages forwarding of data packets.
- The average ratio of the transmitted control bits / delivered data bits can serve as a measure the effectiveness of the protocol in relation to cost management. Note that the calculation should include not only the bits of the routing control packets, but also the header bits of the data packets.
- The average ratio of transmitted data bits and control / delivered data packets can serve measure of pure algorithmic efficiency in terms of bit accounting. This attitude is an attempt for the protocol, the efficiency of access to the channel, such as the cost of such access to channel layer with adversarial access to the transmission medium.

It is also necessary to take into account the network context in which the performance of the protocol is evaluated. Below is list of parameters that have effects on protocol performance:

1) The size of the network, determined by the number of nodes.

2) Connectivity - the average number of neighbors of the network node.

3) Topological rate of change - the speed with which a network's topology is changing

4) The capacity of the channels is the effective channel speed in bits / s, taking into account the losses from multiple access, framing, coding, and so on.

5) The impact of one-way connections - how effective the protocol works in the presence of unilateral connections on the network.

6) Traffic picture - how effectively the protocol adapts to heterogeneity and traffic spikes.

7) Mobility - the impact of long-term and short-term changes in network topology on performance routing protocol.

8) The proportion of "sleeping" nodes and the duration of "sleep" - the effect of the presence of falling asleep and waking up nodes to work protocol.

The MANET protocol must work effectively in a wide range of networks - from small groups to large ones distributed systems with multiple forwarding intervals. In the preceding discussion of the characteristics and parameters it was noted that MANET networks differ from traditional cable networks with many intervals forwarding. (Agandeep et. al, 2012).

In general, the possibilities of MANET networks are attractive, but require the search for technical compromises and difficult decisions. Many different performance problems require the development of new protocols for network management. (Maleki et al, 2003)

5.5 Security Solutions in MANET

This section presents security schemes to deal with the attacks describes in the previous sections.

Zhanget. al(2003)proposed a scheme for intrusion detection in MANET. They proposed distributed and cooperative framework to detect the attack. Every node in the MANET participates in the process of intrusion detection. It detects the sign of intrusion locally and independently and also propagates this information to other nodes in the network.

There is a drawback of distributed and cooperation intrusion detection framework of Zhang et al. (2003) that is due to the limited power capacity that some of the node may behave as selfishly. To eliminate this drawback Huang et.al, (2003) proposed a cluster-based intrusion detection scheme. The whole MANET is organized as a set of clusters where a node is member of at least one cluster. Only one node in a cluster will monitor the intrusion detection. The nodes within a cluster are within the same radio range (Gupta, Shrivastava, & Singh, 2012).

The defense against wormhole attack is done using packet leashes. A Packet leash is additional information attached to the packet to restrict its maximum allowable transmission distance. Two types of leashes exist; a geographical leash that ensures the maximum distance between sender and receiver and a temporal leash bounds the maximum time of packet journey. A receiver examines its time or distance whether it has traveled more than he allowed distance (Chlamtac, Conti, and Liu, 2003)

5.6 Privacy- Preservation in MANET

Secure Multiparty Computation (SMC) is a subject of information security which allows multiple parties to compute some functions of their common inputs without disclosing actual inputs to one another. The problem is that how two millionaire can know who is richer without disclosing individual wealth to one another. There are some solutions available to SMC problem; such as Cryptosystem and Randomization methods. These methods provide privacypreservation during computation. Sometimes data is modified to prevent any possibility of eavesdropping. Some other time the identity of the party is made ambiguous. The mobile ad hoc network can be seen as a multiparty computation paradigm when the mobile node is considered as cooperating party. The Anonypro and extended anonypro protocols can be used to hide the identity of the party. The Secure Sum Protocols can be used for calculating sum, difference, average and other aggregates.

6. Summary

Mobile networks are generally more prone to physical threats than fixed networks with cable connections. To reduce the level of threats in wireless networks, existing protection methods are often used (eg, encryption). In the absence of encryption at the data link layer, one of the most important issues become the authentication of routers before the exchange of control information. Working group examined several levels of authentication, from its complete absence to use full-featured public key management infrastructure. As an additional result several optional authentication modes can be standardized for use in the networks MANET.

Wireless networks are associated with absolutely uncontrolled area between the network endpoints. In a fairly wide space networks, the wireless environment is not controlled. Modern wireless technologies offer a limited set of management scope of network deployment. This allows attackers in direct proximity to wireless structures; produce a number of attacks that were impossible in the wired world. It is noted that self-organizing Ad Hoc networks are vulnerable to the classic types of attacks inherent in all wireless networks, and have their own characteristics. In view of the fact that wireless self-organizing networks do not have a fixed topology, central nodes, stable power supplies, a broadband channel and constant communication of nodes, the task of an attacker to implement a successful attack becomes easier to accomplish, either passive or active attacks using interception (sniffing) and traffic analysis.

References

Amjad, A. H., & Hussam, N. F. (2018). Supernova Optimizer: A Novel Natural Inspired Meta-Heuristic. *Modern Applied Science, 12*(1), 32-50. https://doi.org/10.55399/mas.v12n1p32, 2018

Amjad, A. H., Hussam, N. F., Fatima, E. A. A., & Sandi, N. F. (2017). A Survey about Self-Healing Systems (Desktop and Web Application). *Communications and Network, 9*(1), 71-88, 2017.

Amjad, H., & Hussam, N. F. (2016). An Automated Approach for Software Fault Detection and Recovery. *Communications and Network (CN), 8*(3), 158-169.

Anupama, M., & Sathyanarayana, B. (2011). Survey of Cluster Based Routing Protocols in Mobile Adhoc Networks. *International Journal of Computer Theory and Engineering*, *3*(6), 806.

Barolli, L., Koyama, A., & Shiratori, N. (2003, September). A QoS routing method for ad-hoc networks based on genetic algorithm. In *Database and Expert Systems Applications, 2003. Proceedings. 14th International Workshop on* (pp. 175-179). IEEE.

Carollo, M. E., Farrell, S. M., MacChiano, A., Musselwhite, D. R., & Tarcza, R. P. (2008). *U.S. Patent No. 7,356,818*. Washington, DC: U.S. Patent and Trademark Office.

Chen, S., & Nahrstedt, K. (1999). Distributed quality-of-service routing in ad hoc networks. *IEEE Journal on Selected areas in Communications*, *17*(8), 1488-1505.

Chen, X., Zhai, H., Wang, J., & Fang, Y. (2004). TCP performance over mobile ad hoc networks. *Canadian Journal of Electrical and Computer Engineering*, *29*(1/2), 129-134.

Chlamtac, I., Conti, M., & Liu, J. J. N. (2003). Mobile ad hoc networking: imperatives and challenges. *Ad hoc networks*, *1*(1), 13-64.

Ephremides, A., Wieselthier, J. E., & Baker, D. J. (1987). A design concept for reliable mobile radio networks with frequency hopping signaling. *Proceedings of the IEEE*, *75*(1), 56-73.

Fathi, A., & Taheri, H. (2010, July). Enhance Topology Control Protocol (ECEC) to conserve energy based clustering in wireless ad hoc networks. In *Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on* (Vol. 9, pp. 356-360). IEEE.

Fu, Z., Zerfos, P., Luo, H., Lu, S., Zhang, L., & Gerla, M. (2003, March). The impact of multihop wireless channel on TCP throughput and loss. In *IEEE INFOCOM* (Vol. 3, pp. 1744-1753). INSTITUTE OF ELECTRICAL ENGINEERS INC (IEEE).

Gagandeep, A., & Kumar, P. (2012). Analysis of different security attacks in MANETs on protocol stack A-review. *International Journal of Engineering and Advanced Technology (IJEAT)*, *1*(5), 269-75.

Gummalla, A. C. V., & Limb, J. O. (2000). Wireless medium access control protocols. *IEEE Communications Surveys & Tutorials*, *3*(2), 2-15.

Gupta, N., Shrivastava, M., & Singh, A. (2012). Cluster based on demand routing protocol for mobile ad hoc network. *International Journal of Engineering Research & Technology (IJERT)*, *1*(3), 1-4.

Haas, Z. J., & Deng, J. (2002). Dual busy tone multiple access (DBTMA)-a multiple access control scheme for ad hoc networks. *IEEE transactions on communications*, *50*(6), 975-985.

Haldar, D. (2009). Method and system for controlling scope of user participation in a communication session. U.S. *Patent No. 7,636,750*.

Heenavarshney, P. K. (July 2013). Secure Communication Architecture Based On “BBCMS” Clustering Algorithm for Mobile Adhoc Network (MANET). (IJITEE)ISSN:2278-3075, 3(2).

Himral, L., Vig, V., & Chand, N. (2011). Preventing aodv routing protocol from black hole attack. *International Journal of Engineering Science and Technology (IJEST)*, *3*(5), 3927-3932.

Holland, G., & Vaidya, N. (2002). Analysis of TCP performance over mobile ad hoc networks. *Wireless Networks*, *8*(2-3), 275-288.

Hussein, A. H., Salem, A. O. A., & Yousef, S. (2008, June). A flexible weighted clustering algorithm based on battery power for mobile ad hoc networks. In *Industrial Electronics, 2008. ISIE 2008. IEEE International Symposium on* (pp. 2102-2107). IEEE.

Islam, N., Hossain, M. K., Ali, G. M. N., & Chong, P. H. J. (2016, May). An expedite group key establishment protocol for Flying Ad-Hoc Network (FANET). In *Informatics, Electronics and Vision (ICIEV), 2016 5th International Conference on* (pp. 312-315). IEEE.

Jawandhiya, P. M., Ghonge, M. M., Ali, M. S., & Deshpande, J. S. (2010). A survey of mobile ad hoc network attacks. *International Journal of Engineering Science and Technology*, *2*(9), 4063-4071.

Jhaveri, R. H., Patel, S. J., & Jinwala, D. C. (2012, January). DoS attacks in mobile ad hoc networks: A survey. In *Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on* (pp. 535-541). IEEE.

Johnson, D. B., & Maltz, D. A. (1996). Dynamic source routing in ad hoc wireless networks. In *Mobile computing* (pp. 153-181). Springer, Boston, MA.

Kaliaperumal, B., & Ebenezer, A. (2005, December). Adaptive core based scalable multicasting networks. In *INDICON, 2005 Annual IEEE* (pp. 198-202). IEEE.

Kaur, D., & Kumar, N. (2013). Comparative analysis of aodv, olsr, tora, dsr and dsdv routing protocols in mobile ad-hoc networks. *International Journal of Computer Network and Information Security*, *5*(3), 39.

Kim, D., Min, C. H., & Kim, S. (2004). On-demand SIR and bandwidth-guaranteed routing with transmit power assignment in ad hoc mobile networks. *IEEE transactions on vehicular technology*, *53*(4), 1215-1223.

Konstantopoulos, C., Gavalas, D., & Pantziou, G. (2008). Clustering in mobile ad hoc networks through neighborhood stability-based mobility prediction. *Computer Networks*, *52*(9), 1797-1824.

Kumar, S., Raghavan, V. S., & Deng, J. (2006). Medium access control protocols for ad hoc wireless networks: A survey. *Ad hoc networks*, *4*(3), 326-358.

Leonard, B. A., & Takuo, S. (2003). A Genetic Algorithm (GA) based routing method for Mobile Ad-hoc Networks. *J. Interconnection Networks*, *4*, 257-270.

Leu, J. J. Y., Tsai, M. H., Chiang, T. C., & Huang, Y. M. (2006, September). Adaptive power-aware clustering and multicasting protocol for mobile ad hoc networks. In *International conference on ubiquitous intelligence and computing* (pp. 331-340). Springer, Berlin, Heidelberg.

Luo, Y., Wang, J., & Chen, J. (2006). Algorithm based on mobility prediction and probability for energy efficient multicasting in ad-hoc networks. *Computer research and development*, *43*(2), 231-237.

Maleki, M., Dantu, K., & Pedram, M. (2003, March). Lifetime prediction routing in mobile ad hoc networks. In *Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE* (Vol. 2, pp. 1185-1190). IEEE.

Mishra, R., Singh, A., & Kumar, R. (2016, March). VANET security: Issues, challenges and solutions. In *Electrical, Electronics, and Optimization Techniques (ICEEOT), International Conference on* (pp. 1050-1055). IEEE.

Ni, M., Zhong, Z., & Zhao, D. (2011). MPBC: A mobility prediction-based clustering scheme for ad hoc networks. *IEEE Transactions on Vehicular Technology*, *60*(9), 4549-4559.

Richard, S. W. (1994). TCP/IP Illustrated. *Addison-Welsey Publishing Company*.

Sarkohaki, F., Jamali, S., Fotohi, R., & Balov, J. H. (2012). A simulative comparison of DSDV and OLSR routing protocols. *Australian Journal of Basic and Applied Sciences*, *6*(12), 373-378.

Song, J. H., Wong, V. W., & Leung, V. C. (2004). Efficient on-demand routing for mobile ad hoc wireless access networks. *IEEE journal on selected Areas in Communications*, *22*(7), 1374-1383.

Sundaresan, K., Anantharaman, V., Hsieh, H. Y., & Sivakumar, A. R. (2005). ATP: A reliable transport protocol for ad hoc networks. *IEEE transactions on mobile computing*, *4*(6), 588-603.

Tamilarasan, S. (2012). A quantitative study and comparison of AODV, OLSR and TORA routing protocols in MANET. *International Journal of Computer Science Issues (IJCSI)*, *9*(1), 364.

Tang, J., Xue, G., & Zhang, W. (2005, May). Interference-aware topology control and QoS routing in multi-channel wireless mesh networks. In *Proceedings of the 6th ACM international symposium on Mobile ad hoc* *networking and computing* (pp. 68-77). ACM.

Tang, K., & Gerla, M. (1999). Fair sharing of MAC under TCP in wireless ad hoc networks. In Proceedings of IEEE MMT_99, Venice (I), October.

Temel, S., & Bekmezci, İ. (2013, June). On the performance of flying ad hoc networks (FANETs) utilizing near space high altitude platforms (HAPs). In *Recent Advances in Space Technologies (RAST), 2013 6th International Conference on* (pp. 461-465). IEEE.

Toh, C. K., Cobb, H., & Scott, D. A. (2001). Performance evaluation of battery-life-aware routing schemes for wireless ad hoc networks. In *Communications, 2001. ICC 2001. IEEE International Conference on* (Vol. 9, pp. 2824-2829). IEEE.

Transier, M., Füßler, H., Widmer, J., Mauve, M., & Effelsberg, W. (2004). Scalable position-based multicast for mobile ad-hoc networks. In *BroadWim* (No. LCA-CONF-2004-026).

Tseng, Y. C., Shen, C. C., & Chen, W. T. (2003). Integrating mobile IP with ad hoc networks. *Computer*, *36*(5), 48-55.

Usop, N. S. M., Abdullah, A., & Abidin, A. F. A. (2009). Performance evaluation of AODV, DSDV & DSR routing protocol in grid environment. *IJCSNS International Journal of Computer Science and Network Security*, *9*(7), 261-268.

Wu, H., Zhong, Z., & Hanzo, L. (2010, December). A cluster-head selection and update algorithm for ad hoc networks. In *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE* (pp. 1-5). IEEE.

Xiao, H., Seah, W. K., Lo, A., & Chua, K. C. (2000). A flexible quality of service model for mobile ad-hoc networks. In *Vehicular Technology Conference Proceedings, 2000. VTC 2000-Spring Tokyo. 2000 IEEE 51st* (Vol. 1, pp. 445-449). IEEE.

Xu, K., & Gerla, M. (2002). TCP over an IEEE 802.11 ad hoc network: unfairness problems and solutions. *UCLA Computer Science Department Technical Report—020019*, 1411-1416.

Younis, O., & Fahmy, S. (2004). HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. *IEEE Transactions on mobile computing*, *3*(4), 366-379.

Zhang, Y., Lee, W., & Huang, Y. A. (2003). Intrusion detection techniques for mobile wireless networks. *Wireless Networks*, *9*(5), 545-556.

Copyrights