A SURVEY OF DIFFERENT LETHAL ATTACKS ON MANETs

[1]C.K.Vanamala, [2] Puneet Singhania, [3] Meghana S Kumar

[1]Asst.prof,Dept of Information Science and Engineering,The National Institute of Engineering, Mysore, India; [2]Dept of Information Science and Engineering,The National Institute of Engineering, Mysore, India; [3]Dept of Information Science and Engineering,Sri Jayachamarajendra College of Engineering, Mysore, India.
Email: mala_sanjay@yahoo.com, puneetsinghania2002@gmail.com

ABSTRACT

An Ad Hoc network is a collection of mobile nodes equipped with wireless communication adapters, which dynamically form a temporary network without the need of any existing network infrastructure. The mobile Ad Hoc networks are susceptible to various security threats that cause a disturbance in their development. The central infrastructure is absent which imposes new threats and the services provided by this central infrastructure must now be ensured by the mobile nodes in this new environment. The Ad Hoc networks are often designed for specific environments and communicating nodes may not necessarily entrust upon a fixed infrastructure. They may have to operate with full availability even in difficult conditions where the security solutions applied in more traditional networks may not directly be suitable for safeguarding them.

Keywords – MANET, Ad Hoc Network, Passive attacks, Active attacks, Lethal attacks

1 INTRODUCTION

Mobile Ad Hoc networks consist of mobile platforms which are free to move arbitrarily. This is in contrast with the topology of the existing Internet, where the router topology is essentially static (barring network configuration or router failures). In a MANET, the nodes are mobile and inter-node connectivity may change frequently during normal operation [1]. The characteristics of MANETs such as: dynamic topology, node mobility, provides large number of degree of freedom and self organizing capability which makes it completely different from other network. Due to the nature of MANETs, design and development of secure routing is challenging task for researcher in an open and distributed communication environments [2]. Another novel attack which has recently drawn attention in security prospect is termed as 'detour attack' that aims at conserving the attacker's limited device energy by choosing to forward less data packets. A misbehaved node implementing such lethal attack forces a flow to detour around itself by delaying the propagation of routing messages. Hence, the attacker will reduce the possibility of being selected as a forwarding node and could conserve its energy by evading being selected as a router [3] .Mobile wireless networks are generally more prone to physical security threats than are fixed–cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered. Existing link security techniques are often applied within wireless networks to reduce security threats. As a benefit, the decentralized nature of network control in MANETs provides additional robustness against the single points of failure of more centralized approaches [4]. The proposed paper gives a bird's eye view of what are the possible attacks in Mobile ad hoc networks. Section 2 gives the overall classification of Security Attacks in Ad Hoc and Sensor Networks. Section 3 briefly discusses the classification of attackers. Section 4 discusses the security goals in Sensor networks. Section 5 presents a brief review related to the attacks .Section 6 concludes the paper.Section 7 is acknowledgement of support.

2. Classification of Security Attacks.

Ad Hoc and sensor networks are susceptible to a wide variety of security threats as they are deployed in a hostile environment where they don't get much physical protection. An attack can be Active or Passive.

i) ***Active*****:** In active attacks, malicious attacks are carried out on data integrity along with data confidentiality. It also aims at unauthorised access and usage of resources or disrupting the opponent's communications.

ii) ***Passive attack***: In passive attacks, the attackers do not make any emissions and are mostly against confidentiality of data.

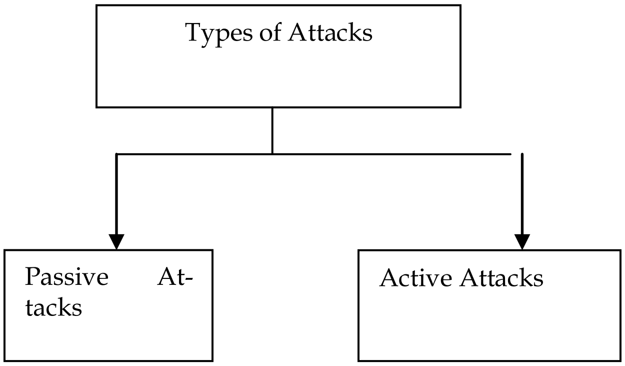

Fig.2.1. Classification of Attacks.

The attacks can be further classified as:

2.1 Classification of Attacks based on general categories.

*2.1.1 Active attacks in general category***:**

- Denial of Service
- Fabrication

  -Node Subversion,-Node malfunction
- Lack of Co-operation

  - Node outage
- Modification

  -Physical attacks, Message corruption
- Impersonation

  -False node, Node replication attacks.
- Eavesdropping

  - Passive Information gathering.
- Other attacks (routing attacks)

  -Spoofed, altered or replayed routing information, Selective forwarding, Sinkhole, Sybil, Wormhole, Hello flood.

*2.1.2 Passive Attacks in general category***:**

These are attacks against privacy monitor and eavesdropping, traffic analysis, camouflages adversaries.

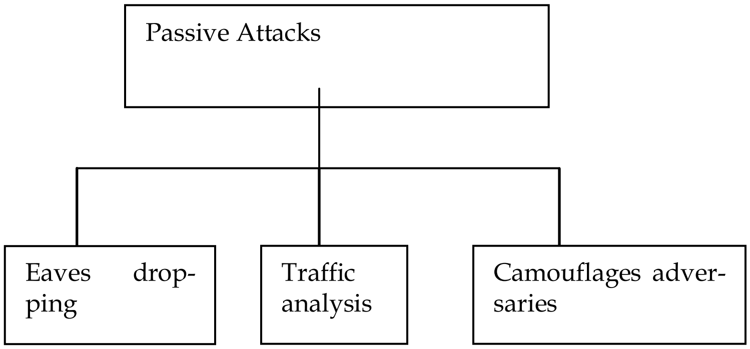

Fig.2.1.2. Classification of passive attacks.

2.2 *Classification of Attacks based on Ad Hoc and sensor networks.*

The Classification of attacks on Ad Hoc and sensor networks can again be classified into

- Passive attacks in Ad Hoc and sensor networks
- Active attacks in Ad Hoc and sensor networks [10].

2.2.1 Passive attacks in Ad Hoc and sensor networks

The attacks against privacy are included in passive attacks.

Sensor networks intensify the privacy problem because large amount of information is made easily available. This is done through remote access. Hence, adversaries are not needed to be physically present to maintain surveillance. Direct site surveillance is used to collect the information from sensor networks. Information can be collected at low-risk in anonymous manner. Attacks against privacy can be subdivided into:

i*) Monitor and Eavesdropping*:

Eavesdropping is the act of secretly listening to the private conversation of others without their consent, as defined by Black's Law Dictionary [19]. Eavesdropping can be done over telephone line (wiretapping), email, instant messaging and other methods of communication which are considered private. It is a network layer attack consisting of capturing packets from the network which is transmitted by other's computers and reading the data content in search of sensitive information like passwords, session tokens or any kind of confidential information. Tool for performing these attacks are Network sniffers. They perform the task of collecting packets on the network and, depending on the quality of the tool, analyse the collected data like protocol decoders or stream reassembling.

ii) Traffic analysis:

Traffic analysis can be defined as the process of intercepting and examining message so that information patterns in communications can be deduced. It can perform even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed for military intelligence and is common in computer security.

Various techniques used for traffic analysis by attackers are:

- *Traffic analysis at the physical layer***:** Here, only the carrier is sensed and the traffic rates are analyzed for the nodes at a location.
- *Traffic analysis in MAC and higher layers***:** MAC frames and data packets can be demultiplexed and headers can be analyzed. This can reveal the routing information, topology of the network and friendship trees.
- *Traffic analysis by event correlation:* Events like detection in a sensor network or transmission by an end user can be correlated with the traffic and more detailed information, e.g. routes, etc., can be derived.
- *Active traffic analysis:* Traffic analysis can also be conducted as an active attack. For example, a certain number of nodes can be destroyed, which stimulates self organization in the network, and valuable data about the topology can be gathered.

iii) Camouflage adversaries:

An adversary may compromise a sensor node in a WSN and later on use that node to masquerade as a normal node in the network. This camouflaged node may advertise false routing information and attract packets from other nodes for further forwarding. After the packets start arriving at the compromised node, it starts forwarding them to strategic nodes where privacy analysis on the packets may be carried out systematically [20].

2.2.2. *Active Attacks in Ad Hoc and sensor networks*

The following are the active attacks in Ad Hoc and sensor networks:

i) Masquerade, Replay, Message modification
- Integrity
- Unauthorized access
- Confidentiality
- Privacy

ii) Denial of Service
- Physical layer
- MAC layer
- Network layer
- Transport layer
- Application layer

iii) Physical
- Destruction
- EMP
- Tampering

iv) Misbehaving
- Selfishness
- Attacks against charging scheme

Other attacks which can be listed as active attacks are DOS, Node subversion, Node malfunction, Node outage, Physical attacks, Message corruption, false node, Node replication attacks, Passive information gathering, Routing attacks in sensor networks.

1. Denial of service (DOS) attacks:

DOS attacks are the attacks which prevent the normal use or management of communication the services and may take the form of either a targeted attack on a particular service or a broad incapacitating attack. For example, a network can be considered which may be flooded with messages that cause a degradation of service or possibly a complete collapse. Another example that can be considered is rapid and repeated requests to a web server in which legitimate access to others is barred.DOS attacks are frequently reported for internet-connected services. Perpetrators of DOS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name servers. This technique has now seen extensive use in certain games, used by server owners, or disgruntled competitors on games. Increasingly, DOS attacks have also been used as a form of resistance. Richard Stallman has stated that DOS is a form of 'Internet Street Protests' [11]. The term is generally used relating to computer networks, but is not limited to this field; for example, it is also used in reference to CPU resource management [12].

2) Node Subversion:

In node subversion, when a node is captured, it may reveal its information. This may include disclosure of cryptographic keys and thus jeopardizes the whole sensor network. In this, the key is stored on the sensor so that when it is captured, the information or key stored on it might be obtained by an attacker.

3) Node malfunction:

A large number of portable sensor nodes are used in WSN, due to which the probability of sensor node failure gets increased .It has affected the reliability and efficiency of WSN. It is essential to detect failed or malfunctioning sensor node to maintain the high quality of WSN. The failure of sensor node results either because of communication device failure or battery, environment and sensor device related problems. There is a proposed method to detect node malfunction which uses the round trip delay (RTD) time for estimating the confidence factor which is used to detect the failed or malfunctioning sensor node. Hardware based simulation result indicates the easy and optimized way to detect failed or malfunctioning sensor node in symmetrical WSN.

4) Node outage:

Node outage can be defined as the situation that occurs when a node stops its function. The sensor network protocols should be robust enough to moderate the effects caused by node outages by providing an alternate route when a cluster leader stops functioning.

5) Physical Attacks:

Sensor node hardware has some conceivable attacks which do not really fit the accepted usage. In order to avoid this terminology problem, those attacks that are regarded physical attacks are called and this term is used to refer to all attacks which require direct physical access to the sensor node. Sensor networks are typically deployed in hostile regions where small form factor of the sensors coupled with the unattended and distributed nature of their deployment makes them vulnerable to physical attacks. The sensors are destroyed permanently by them and the losses can't be reversed.

6) Message corruption:

Any modification of the content of a message by an attacker compromises its integrity [13].

7) False node:

The false nodes are the nodes which can inject false data during data aggregation. Data aggregation is implemented in WSN so that data redundancy can be eliminated. A node is added by an adversary due to which the injection of malicious data is caused. It could spread to all nodes and could destroy the whole network or take over the network on behalf of an adversary.

8) Node Replication Attacks:

Node replication can be said to be successfully implemented when it starts with how well the initial replication of data and the subsequent incremental daily replication are planned during normal operations. It is to be ensured that appropriate, well tuned hardware resource is dedicated to the task. Increased amounts of memory and CPU are required. The database and its logs must be appropriately sized so that it can be ensured that the transactions can proceed till completion. It requires a dedicated network with enough bandwidth to handle the amount of data intended to replicate. We consider the node replication attack, which is an application-independent attack unique to wireless sensor networks. The attack makes it possible for an adversary to prepare her own low-cost sensor nodes and induce the network to accept them as legitimate ones [14].

9) Passive Information Gathering:

'Passive' refers to the techniques that either do not connect to a system owned or managed by the organisation (so that they would be unaware of any such access to information from the organization systems) which is commonly available and would not normally ever be associated a precursor to future attacks or via the increasingly numerous online security analysis websites. The techniques used to uncover this leaked information are commonly referred to as "Passive Information Gathering" – and they form a vital (and often overlooked) role in any quality penetration test or security assessment [15].A lot of important information can be passively harvested and that can be subsequently used in a direct attack or to reinforce other attacks targeted at an organisation. Depending upon the source, information such as current service patching levels, internal network architecture layout and account details can be easily obtained and the level of detail of information, this information leakage can be rectified by an organisation simply and quickly.

10) Routing attacks in sensor networks

Routing attacks can be defined as the attacks which are acting on the network layer. Many attacks act on the network layer. Many attacks happen while routing the messages. They are as follows:

a) Spoofed, altered and replayed routing information:

In this, every node acts as a router so an unprotected Ad Hoc routing is susceptible to these types of attacks. This can:

- Directly affect routing information
- Create routing loops
- Generate false error messages
- Extend or shorten service routes
- Increase end to end latency

b) Selective forwarding:

In a black hole attack, compromised node drops all the packets forwarding through it. A special case of black hole attack is selective forwarding attack, where compromised node drops packets selectively, which may deteriorate the network efficiency[16]. Selective forwarding attacks are the attacks which may corrupt some mission critical applications such as military surveillance and forest fire monitoring. The malicious nodes behave like normal nodes in most time but selectively drop sensitive packets such as a packet which reports the movement of opposite forces. A multihop acknowledgement technique can be used for the detection of selective forwarding to launch alarms by obtaining.

c) Sybil Attacks:

The Sybil attack in computer security is an attack wherein a reputation system is subverted by forging identities in peer-to-peer networks. It is named after the subject of the book Sybil, a case study of a woman diagnosed with dissociative identity disorder [17].The reputation system of a peer to peer network is subverted by an attacker by creating a large number of identities which are pseudonymous used to gain a disproportionately large influence .The susceptibility of a reputation system accepts inputs from entities that do not have a chain of trust linking them to a trusted identity and whether the reputation system treats all entities identically.

d) Wormhole attacks:

Being a broadcast medium, innate advantage is offered by a wireless medium to any adversary who intends to spy in or disrupt the network .Wormhole attacks are one of the most easy to deploy for such an adversary. For launching a wormhole attack, an adversary connects two distant points in the network using a direct low-latency communication link called as the wormhole link. The wormhole link can be established by a variety of means, e.g., by using a ethernet cable, a long-range wireless transmission, or an optical link. Once the wormhole link is established, the adversary captures wireless transmissions on one end, sends them through the wormhole link and replays them at the other end [18].

e) HELLO flood attacks:

The protocol requires the nodes to broadcast HELLO packets to announce themselves to their neighbours, and a node that receives such a packet may assume that it is within (normal) radio range of the sender. However, in some cases, this assumption may be false; sometimes a laptop-class attacker who is broadcasting routing or other information with large enough transmission power could convince every other node in the network that the attacker is its neighbour.

f) Detour attacks-Routing Detour:

The attacker also intercepts the SOAP message during this attack, but instead of altering the SOAP body, additional routing information is added to the SOAP Header. The altered message is then passed to the new intermediary(s). When new intermediaries are added, it can be assumed that these intermediaries are under the control of the attacker. A Malicious Morphing attack is usually performed by malicious intermediaries. When an intermediary is bypassed , certain operations on the SOAP message are omitted which means that certain changes of the SOAP message that are unwanted to the attacker are left out. For example, the payment-operation could be considered one of these functions.

2.3 Classification of attacks based on individual layers:

These attacks on MANETs challenge the mobile infrastructure in which nodes can leave and join easily with dynamic requests and no static path of routing. Attacks on individual layer are as under:

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

2.4 Some more attacks in MANETS:

TCP attacks are the major problem faced by Mobile Ad hoc Networks (MANETs) due to its limited network and host resources. Attacker trace back is a promising solution which allows a victim to identify the exact location of the attacker and hence enables the victim to take proper countermeasure near attack origins, for forensics and to discourage attackers from launching the attacks. However, attacker trace back in MANET is a challenging problem due to dynamic network topology, limited network and host resources such as memory, bandwidth and battery life [5]. Identity spoofing, link withholding, link spoofing, replay attack, wormhole attack and colluding misrelay attack are some of the problems which has been discussed earlier. Link spoofing, wormhole attacks and colluding misrelay attacks have not yet been solved. Detour attack has not been addressed in any of the works. Identity spoofing is related to brute force login attempts, digital certificate theft and forgery. Replay attacks degrade severely MANET performance. This attack is performed by interception and retransmission of valid signed messages

[6].

3. Classification of attackers

Attackers can be categorized according to many criteria. The classification of attackers is based on the characteristics shown in below: emission, location, quantity, motivation, rationality and mobility. First, an attacker can be passive or active. Active attacks are carried out by active attackers and passive attacks by passive attackers. An attacker can be an insider or an outsider. There may be a single attacker or more than one. When there are multiple attackers, they can collaborate with each other, which can be considered a more difficult case to defend against. In Hu *et al.* (2005) active attackers are denoted Active-*n-m*, where *n* is the number of insider nodes, and *m* is the total number of insider and outsider nodes. They then propose an attacker hierarchy with increasing strength as follows:

Active-0-1: the attacker owns only one outsider node.

Active-0-*x*: the attacker owns *x* outsider nodes.

Active-1-*x*: the attacker owns *x* nodes and only one of them is an insider.

Active-*y*-*x*: the attacker owns *x* nodes and *y* of them are insiders.

Note that in this hierarchy all the nodes represent a single attacker. Therefore, they are
supposed to collaborate.

3.1 Characteristics of the attackers

- *Emission* – Active, Passive.
- *Location*– Insider, Outsider.
- *Quantity*– Single, Multiple, Coordinating multiple.
- *Motivation*– Confidentiality, Integrity, Privacy, Unauthorized access, DOS, Selfishness, Charging, Rewarding.
- *Rationality*– Naïve, Irrational, Rational
- *Mobility*– Fixed, Mobile.

4. Security Goals

Security is the quality or state of being secure to be free from danger. A successful organization should have the following multiple layers of security.

- *Physical security*- it is to protect physical items, objects or areas from unauthorized access and misuse.
- *Personal security*- to protect the individual or group of individuals who are authorized to access the organization and its operation.
- *Operations security*- To protect the details of a particular operation or series of activities.
- *Communications security*- to protect communications media, technology and content.
- *Network security*- To protect networking components, connections and contents.
- *Information security*- To protect information assets.

The goal of security is to provide security services to defend against all the kinds of threat explained in this paper. Security services include the following:

• **Authentication:** This ensures that the other end of a connection or the source of a packet is the node that is claimed.

• **Access control:** This prevents from unauthorized access to resources.

• **Confidentiality:** It protects the overall content in a message. Confidentiality can also be required to prevent an attacker from doing traffic analysis.

• **Privacy:** This prevents the attackers from obtaining information that may have private content. The private information may be obtained through the analysis of traffic patterns, i.e. frequency, source node, routes, etc.

• **Integrity:** It ensures that a packet is not altered during transmission.

•**Authorization:** It authorizes another node to update information (import authorization) or to receive information (export authorization). Typically, other services such as integrity and authentication are used for authorization.

• **Anonymity:** It conceals the source of a packet or frame. It is a service that can help with data privacy and confidentiality.

• **Nonrepudiation:** This proves the source of a packet. . Nonrepudiation prevents the source from denying that it sent a packet. In authentication, the source proves its identity.

• **Freshness:** This attack ensures that a malicious node does not resend previously captured packets.

• **Availability:** This mainly targets DOS attacks and it is the ability to sustain the networking functionalities without any interruption due to security threats.

• **Resilience to attacks:** This is required to sustain the network functionalities when a portion of nodes is compromised or destroyed.

5. Related Work

Wenjia Li and Anupam Joshi [7] have discussed about two kinds of popular security techniques in the mobile ad hoc network, which are intrusion detection techniques and secure routing techniques. In each of the security schemes, several specific methods are pointed out and compared with each other.

Muhammad Arshad Ali and Yasir Sarwar [8] proposed a thesis whose aim of was to discuss different aspects of security in MANET; firstly discuss multi-layer intrusion detection technique in multi hop network of Mobile ad hoc network; secondly discuss security problems related between multi hop network and mobile nodes in Mobile ad hoc network. The second most important aspect of the thesis was to implement some of the solutions; firstly they did comparative study of different routing protocol (AODV, DSR and TORA); secondly they implemented security threats within MANET network like intruder behavior, tapping and integrity; thirdly they also implemented MANET link layer and network layer operations with respect to information security.

Djamel Djenouri and Nadjib Badache [9] has presented different kinds of attacks on routing protocol and they have classified and discussed the proposed solutions. They have also presented attacks and misbehavior on data forwarding which have received relatively less attention in literature, they think securing data forwarding is a fertile field of research. Regarding the medium access layer, they have presented the non-respect on the channel access misbehavior that can affect hugely the network efficiency, and they have presented and discussed the lonely solution proposed. In their discussion, they have shown how this solution may accuse wrongly a well-behaving node, and how it is unable to detect what they have called cooperative misbehavior. They have also presented the key distribution issue that can be an underlying mechanism for securing both lower and upper layers, and finally Intrusion Detection Systems (IDSs) that are essential when preventive measures fail have been presented.

Richard Stallman has stated that DOS is a form of 'Internet Street Protests’ [11].

He describes that perpetrators of DOS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name servers. This technique has now seen extensive use in certain games, used by server owners, or disgruntled competitors on games. Increasingly, DOS attacks have also been used as a form of resistance.

6. Conclusions

The mobile adhoc networks are susceptible to various security threats that cause a disturbance in their development. The central infrastructure is absent which imposes new threats and the services provided by this central infrastructure must now be ensured by the mobile nodes in this new environment. The ad hoc networks are often designed for specific environments and communicating nodes may not necessarily entrust upon a fixed infrastructure. They may have to operate with full availability even in difficult conditions where the security solutions applied in more traditional networks may not directly be suitable for safeguarding them. Security is an important feature for the deployment of Ad Hoc and Sensor Networks. This paper summarizes the attacks and their classifications in Ad Hoc and Sensor Networks .The challenges of Ad Hoc Networks are also briefly discussed. This paper motivates future researchers to come up with smarter and more robust security mechanisms and make their network safer.

7. Acknowledgment

This work was supported by Association of Computer Engineers, CS Division, NIE, Mysore, Karnataka.

8. REFERENCES

[1] Mobile Ad hoc networking,Carlos de Morais Cordeiro and Dharma P. Agrawal,OBR Research Center for Distributed and Mobile Compu-

ting,ECECS,University of Cincinnati,Cincinnati,OH 45221-0030 – USA,{cordeicm,dpa}@ececs.uc.edu.

[2] An Overview of security Problems in MANET, Kuldeep Sharma, Neha Khandelwal, Prabhakar M.

[3] Guang, L., Assi, C., (2006) Interlayer Attacks in Mobile Ad Hoc Networks, Springer.

[4] T. Clausen, P. Jacquet, Optimized Link State Routing Protocol (OLSR), 2003.

[5] Nishanth, N and Venkataram, Pallapa (2011) *Mobile agent based TCP attacker identification in MANET using the traffic history (MAITH).* In: IEEE 13th International Conference on Communication Technology (ICCT), 25-28 Sept. 2011, Jinan.

[6] Sadeghi, M., (2012), Analysis of Wormhole Attack on MANETs Using Different MANET Routing Protocols, IEEE.

[7] Security Issues in Mobile Ad Hoc Networks-A Survey,Wenjia Li and Anupam Joshi, Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore Country.

[8] Muhammad Arshad Ali and Yasir Sarwar, (March 2011) Security Issues regarding MANET(Mobile Ad Hoc Networks): Challenges and Solutions, Master Thesis, Computer Science, Thesis no: MCS-2011-11 ,

[9] Djamel Djenouri and Nadjib Badache, (February 2004), A Survey on Security Issues in Mobile Ad Hoc Networks, , LSI-TR0504.

[10] a b c d e Internet Engineering Task Force RFC 2828 Internet Security Glossary.

[11] "The Philosophy of Anonymous". Radicalphilosophy.com. 2010-12-17. Retrieved 2013-09-10.

[12] Shabtai, A.; Fledel, Y.; Kanonov, U.; Elovici, Y.; Dolev, S.; Glezer, C. (March–April 2010). "Google Android: A Comprehensive Security Assessment". IEEE Security & Privacy Magazine 8 (2): 35–44. doi:10.1109/MSP.2010.2. edit PDF.

[13] http://electronicsforu.com/electronicsforu/circuitarchives/ Cryptography Mechanisms For access Control in Wireless Sensor Networks.

[14] Network Computing and Information Security (NCIS), 2011 International Conference on (Volume:2), Print ISBN: 978-1-61284-347-6,INSPEC Accession Number:12116968,Conference Location :Guilin,Digital Object Identifier :10.1109/NCIS.2011.130.

[15] http://www.technicalinfo.net/papers/PassiveInfoPart1.html

[16] Devices and Communications (ICDeCom), 2011 International Conference,Print ISBN: 978-1-4244-9189-6, INSPEC Accession Number:11887750,Conference Location :Mesra,Digital Object Identifier :10.1109/ICDECOM.2011.5738547.

[17] http://www.npr.org/2011/10/20/141514464/real-sybil-admits-multiple-personalities-were-fake

[18] http://www.wings.cs.sunysb.edu/~ritesh/wormhole.html

[19] Garner, p. 550.

[20] Wireless Sensor Networks: Current Status and Future Trends, edited by Shafiullah Khan, Al-Sakib Khan Pathan, Nabil Ali Alrajeh.