British Journal of Mathematics & Computer Science
5(2): 247-261, 2015, Article no.BJMCS.2015.017
ISSN: 2231-0851

SCIENCEDOMAIN *international*
www.sciencedomain.org

Towards a Taxonomy of MANETs Attacks: Attack Attributes-based Taxonomy (AABT)

Noureldien A. Noureldien[1*]

[1]*Department of Computer Science, University of Science and Technology, Omdurman, Sudan.*

Article Information

DOI: 10.9734/BJMCS/2015/13529
Editor(s):
(1) Kai-Long Hsiao, Taiwan Shoufu University, Taiwan.
(2) Kewen Zhao, Institute of Applied Mathematics & Information Sciences, Department of Mathematics, University of Qiongzhou, Sanya, P.R. China.
Reviewers:
(1) Shrikant Upadhyay, Electronics & Communication Engg. Dept., Cambridge Institute of Technology, Ranchi, India.
(2) Anonymous, Jackson State University, USA.
(3) Farouk Yalaoui, Department of Industrial Systems Engineering, Troyes University of Technology, France.
Complete Peer review History: http://www.sciencedomain.org/review-history.php?iid=726&id=6&aid=6734

Original Research Article

Received: 21 August 2014
Accepted: 08 October 2014
Published: 30 October 2014

Abstract

Mobile Ad hoc Networks (MANETs) find a rapid increase of applications and interest. The vulnerabilities of MANETs make the security issue a major concern for researcher and practitioners. MANETs attacks are often described and classified differently, resulting in confusion in what a particular attack actually is and how attacks can be categorized.

Generally, the purpose of attack taxonomy is to provide a useful and consistent means of classifying attacks. A well defined taxonomy will allow previous knowledge to be applied to new attacks as well as providing a structured way to view such attacks.

This paper proposes a new taxonomy to MANETs attacks. The taxonomy is aimed to provide means to create attack categories, to enable highlighting similarities between attacks and to be useful in identifying attack-related detection and prevention countermeasures.

The taxonomy is based on attack attributes. Every attack is characterized by a unique vector of attributes values, where each attribute define a specific attack property which may have different values. The taxonomy uses six attributes; the legitimacy of attacking node/s, the number of nodes participating in the attack, MANETs vulnerabilities utilized by the attack, the network resources exploited by the attacking node/s, the targeted victim and finally, the network security service compromised by the attack.

The analysis of some well known attacks shows the capability of the proposed taxonomy in describing and categorizing these attacks as taxonomy vectors.

Keywords: MANETs attacks, attacks classification, attacks taxonomy, attack attributes.

**Corresponding author: noureldien@hotmail.com;*

1 Introduction

In a mobile ad hoc network (MANET), a collection of mobile devices called wireless hosts equipped with wireless network interfaces form a temporary network without aid of any fixed network infrastructure or centralized administration. Accordingly, MANET is referred to as an infrastructureless network. MANTET mobile nodes in the network dynamically set up paths among themselves to transmit packets. In a MANET nodes within each other's wireless transmission ranges can communicate directly; however, nodes outside each other's range have to rely on some other nodes to relay messages. Thus, a multi-hop data transmission is occurring, where several intermediate hosts relay the packets sent by the source host before they reach the destination host. Every node functions as a router and the success of communication is highly depending on other nodes' cooperation.

Nowadays, there are various MANET applications such as military tactical communication, medical services, law enforcement operations, commercial and educational use, and sensor networks [1,2].

Unlike the conventional network, a MANET is characterized by having a dynamic, continuously changing network topology due to mobility of nodes [3]. This feature makes it difficult to perform routing in a MANET compared with a conventional wired network. Therefore to provide effective functionality the traditional routing protocols was modified to meet these special needs. And thus many dedicated protocols have been invented such as AODV [4], DSR [5].

Also, in MANETs, nodes within each other's wireless radio transmission ranges can communicate directly; however, nodes outside each other's range have to rely on some other nodes to relay messages [3]. Thus, the success of communications is highly depends on other nodes' cooperation.

Another characteristic of a MANET is its resource constraints, that is, limited bandwidth and limited battery power. This characteristic makes routing in a MANET an even more challenging task. Therefore, early work in MANET research focused on providing routing service with minimum cost in terms of bandwidth and battery power.

The above weaknesses of MANETs make it highly susceptible to many attacks. For example, routing messages defined by routing protocols, which are an essential for constructing a route from source to the destination can be subject for malicious acts such as modifications, fabrications and dropping.

To achieve security services such as confidentiality, authentication, integrity, availability, access control, and non-repudiation in MANETs, a comprehensive study to MANETs attacks is obligatory.

Many research works define and classify MANTEs attacks from different perspectives, but a few out of this research work proposes a taxonomy to MANETs attacks. Taxonomies provide a deep understanding to attacks and facilitate developing attack-related detection and prevention techniques. Many requirements and characteristics have been defined in the literature for a good taxonomy, these includes [6];

Accepted: The taxonomy should be detailed and structured so that it can be generally approved.

Comprehensible: The taxonomy has to be easily understood.

Completeness/Exhaustive: The taxonomy should classify all possible attacks and provide categories accordingly. Completeness can be justified through successful categorization of existing actual attacks.

Deterministic: The procedure used in classification must be clearly defined.

Mutually exclusive: The taxonomy must categorize each attack into, at most, one category.

Unambiguous: The taxonomy must define each category clearly so that there is no ambiguity with respect to attack categorization.

Useful: A useful taxonomy will be able to be used in the security industry and particularly by incident response teams.

Currently a large number on MANETs attacks are exits, and despite of the large research work in classifying MANET attacks, the number of works aimed to introduce a certain order to MANETs attack is reduced [7]. Most of research work proposes a theoretical classification that lack behind providing a base for building an attack-related detection and prevention systems.

This paper proposes a novel taxonomy approach to MANETs attacks. The novel taxonomy is an Attack Attributes Based Taxonomy (AABT); it consists of six classification attributes which provide a holistic taxonomy that provides a base for building attack-related detection systems. The first attribute specify the legitimacy of attacking node/s. The second attribute specify the number of nodes participating in the attack, the third attribute identify MANETs vulnerabilities utilized by the attack. The network resources exploited by the attacking node/s define the forth attribute. The fifth attribute characterize the targeted victim and finally, the network security service compromised by the attack, i.e. the attack goal, classifies the sixth attribute.

Following this introduction, the paper is organized as follows. Section 2 overviews previous MANETs attacks taxonomy and classifications research work, and Section 3 presents the AABT taxonomy; Section 4 provides examples of AABT taxonomy attack vectors and finally, Section 5 concludes the paper.

2 Previous Attacks Taxonomies and Classifications

Two of the early taxonomies in the security field were the Protection Analysis (PA) taxonomy [8] and the Research in Secured Operating Systems (RISOS) [9]. Although these two taxonomies were centered on vulnerabilities exploited by attacks rather than the attacks themselves, they provide a good background for researchers working on attacks taxonomies.

In [10] a taxonomy of Unix vulnerabilities is proposed, in which the underlying vulnerabilities to define a classification scheme that constitute six variables, namely, nature, time of introduction, exploitation domain, effect domain, minimum number and source.

In [11] an approach to a taxonomy of computer and network attacks was suggested. The approach taken is a process-based approach that takes into account factors such as attacker motivation and objectives. A computer attacks taxonomy called VERDICT (Validation Exposure Randomness

Deallocation Improper Conditions Taxonomy) is proposed in [12], it is based on the characteristics of attacks. Instead of a tree-like taxonomy, he proposed using four characteristics of attacks, namely, improper validation, improper exposure, improper randomness and improper deallocation.

The approach in [6] proposes a computer attacks taxonomy that works by using the concept of dimensions. The taxonomy proposes four dimensions for attack classification. The first dimension is used to categorize the attack into an attack class that is based on the method by which an attack reaches its target. The attack target is covered in the second dimension. The third dimension covers the vulnerabilities and exploits, if they exist, that the attack uses. The fourth dimension takes into account the possibility for an attack to have a payload or effect beyond itself.

2.1 MANETs Attacks Taxonomies

The above taxonomies are general security attack taxonomies. For MANETs attacks, the literature presents a few taxonomies and a wide range of attacks classification proposals. One widely used classification classifies MANETs attacks into two major categories, namely passive attacks and active attacks [13,14]. A passive attack obtains data exchanged in the network without disrupting the operation of the communications, while an active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of a MANET.

The concept of anomalous basic events was used to study MANET attacks in [15], where an anomalous basic event is a basic event that does not follow the system specification. They use the concept in order to capture the characteristics of basic attack components. They identify an anomalous basic event by two components, its target and operation. Targets include: routing messages, data packets and routing table (or routing cache) entries. Possible attack operations on these targets are identified by examining the well-known security goals: Confidentiality, Integrity and Availability.

The major drawback of this approach is that it is possible that some attacks do not generate any anomalous basic events. For example, an attack may involve elements from a different layer that the system specification does not describe, or it may involve knowledge beyond a single node. A Wormhole attack is an example of the first case, where two wireless nodes can create a hidden tunnel through wires or wireless links with high transmission rate.

A classification of MANETs attacks based on using a hybrid model of OSI and TCP/IP called the Tanenbaum model was proposed [16], which has five layers: application, transport, network, data link and physical layer. Another classification categorize the present existing MANETs attacks into two broad categories: data traffic attacks and control traffic attacks based on the packet's type exploited by the attack [17].

One more approach classifies attacks according to the target security service, i.e. confidentiality, integrity and availability [18], and a criterion that includes the goal of the attack is used to classify MANETs DOS attacks [19,20].

A recent taxonomy in [7], provide a taxonomy for MANETs attacks that is based on a root of all MANETs attacks and from that root successive groups are obtained for known attacks until each specific variant of attack is derived. The criteria used to define the 3-level tree each of the

taxonomy are; action of attackers, effect of the attack, procedure of the attack and function or service attacked.

3 The Attack Attribute Based Taxonomy (AABT)

In order to formulate taxonomy of MANETs attacks we observe the characteristics of the attack itself and the effect it has on the victim. These characteristics and effects define the attack attributes. Accordingly a MANET attack will be classified based on a group of attributes it have. The following attributes are used in the taxonomy.

- Legitimacy of attacking node/s.
- Number of nodes participating in the attack.
- Utilized MANETs vulnerabilities (UMV).
- Exploited network resources (ENR).
- Targeted victim (TV), and
- Compromised security service (CSS)

The taxonomy defined each attack as a vector of six attribute values. The value assigned to an attribute can be a compound of more than one single value of attribute values. Each of the above classification criteria or attributes is discussed below in a separate subsection, and Fig. 1 summarizes the taxonomy.

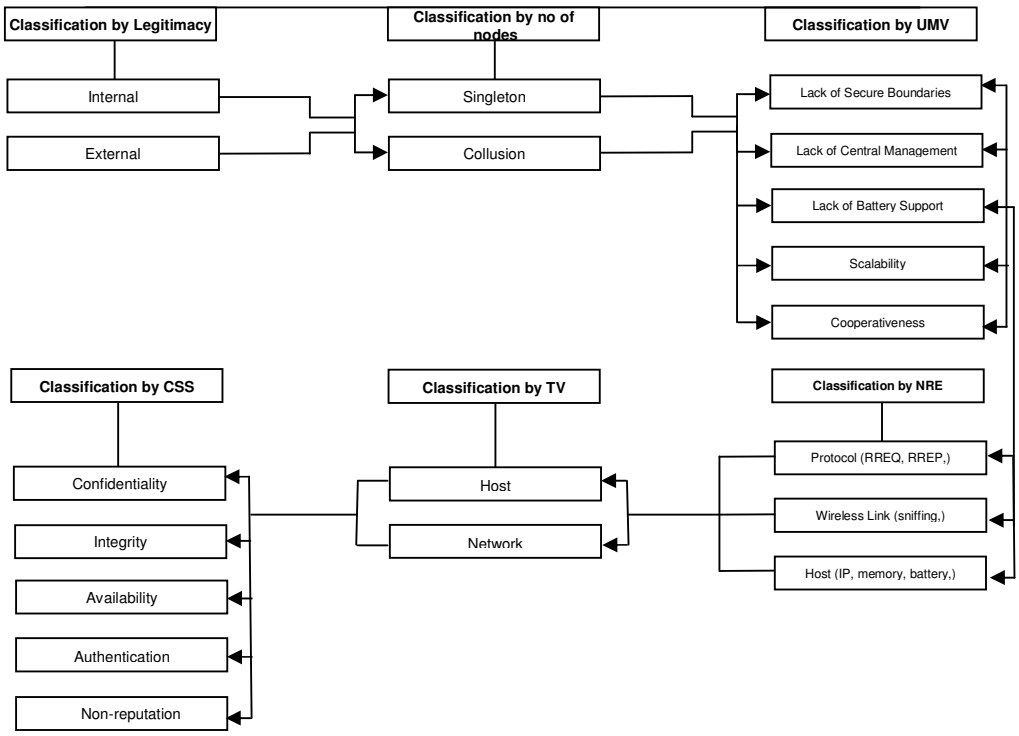

Fig. 1. Attack attributes base taxonomy

3.1 Classification by Attacking Node Originality

MANETs attacks can be classified in two types; external and internal [21]. External attacks are attacks in which the attacker, using unauthorized node, aims to cause congestion, propagate fake routing information or disturb nodes from providing service. In internal attacks the attacker, using either a legitimate node or a compromised node, wants to gain the normal access to the network and participate in the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors.

Based on the legitimacy of attacking node/s we distinguish between the following attribute values:

- External attacking node/s
- Internal attacking node/s

External nodes are those nodes that are not primary part of the legitimate MANET, but they exploit the mobility and lack of authenticity to be part of the network to initiate malicious events, while internal nodes are legitimate MANET nodes, but they initiate malicious events either consciously or because they are compromised by other node/s.

3.2 Classification by Number of Attacking Nodes

In MANETs, attacks are either launched by single host, or by collaborative hosts. Examples for single node attacks include; routing cache poisoning attack [22], rushing attacks [23], hello flood attack [24] and blackhole attack[25,26]. Collaborative attacks include wormhole attack [27], Byzantine attack [28] and blackhole attack [29,30].

Based on the number of nodes involved in the attack, we differentiate between the following attribute values:

- Singleton attack;
- Collusion attack.

In a singleton attack only one node is in participation while in a collusion attack multiple nodes work in collusion to achieve a malicious act in a MANET.

3.3 Classification by Exploited MANET Vulnerability

MANET vulnerabilities mean a limitation and weak points in this network security system. Any attack takes advantage of one or more of these vulnerabilities. Based on the MANET vulnerability that is exploited by the attack, we differentiate between the following attribute values:

- Lack of Secure Boundaries
- Lack of Central management
- Lack of battery support
- Scalability
- Cooperativeness

Lack of secure boundaries is due to the fact that, in MANET there is no clear secure boundary, nodes have the choice to join and move in the network freely [31,32], so the malicious node can join automatically when it's in the radio range. Consequently the attacks can come from all directions.

Lack of centralized management is one of the significant vulnerabilities that results from the similar behavior an operation of MANET all nodes. Consequently, MANET has no centralized administration entity which is responsible of monitoring the traffic in the network [31][33].

Limitation of resources in MANET is due to different types of nodes such as laptops, PDAs and mobile phones. These devices have limited resources such as memory and battery [34]. This makes MANET vulnerable to some attacks; for example sleep deprivation and DoS attacks.. The limitation of resources can be a serious challenge to perform cryptographic security that requires computation-intensive tasks.

Scalability problem in MANET is a consequence of the nature of MANET that does not a particular predefined scale due to randomness of topology changes [35]. This characteristic makes some of powerful traditional security mechanisms inapplicable in MANETs.

The routing operation in MANET depends on cooperation between connected nodes to communicate in trusted environment [36]. For example the use of intermediate node that can assists the sender when the destination is not in the range of the sender. Some nodes exploit this need to cooperative to make a malicious behavior in the network. For example, a node can pose as a neighbor to other nodes and participate in collective decision-making mechanisms, possibly affecting networking significantly.

3.4 Classification by Exploited Network Resource

Each attack exploits a network resource weakness to launch an attack. Based on the resource vulnerability exploited during an attack, we differentiate between the following attribute values.

- Routing protocol
    - RREQ
    - RREP
    - Routing Table
    - Bypassing Protocol Rule
- Wireless links
    - Sniffing
    - Broadband
- Wireless hosts
    - IP address
    - Memory
    - Battery
    - OS

3.5 Classification by Targeted Victim

Each attack targeted a specific node in the network, multiple nodes or the whole network. Based on the targeted wireless device we differentiate between the following attribute values:

- Single node targets (Host), and
- Multiple nodes or network targets (Network).

In a single node target attacks, the goal of attacking node/s is to compromise security of a specific node. Examples of such attacks includes eavesdropping traffic originated from specific IP address, gaining illegal access to a node resources, denial of access to a certain node, ..etc.

In a network target attacks, the goal of the attacking node/s is to compromise security and network presence of multiple nodes or the whole network. Examples of attacks target network presence include attacks that force network partitioning and isolation, and attacks that target the whole network includes traffic analysis and monitoring attacks.

3.6 Classification by Compromised Network Security Requirements

Each attack attempts to achieve a specific malicious goal that violates one of the network security characteristics. Based on the security characteristic violated by the attack we differentiate between the following attribute values:

- Confidentiality
- Integrity
- Availability

Availability is defined according as "ensuring timely and reliable access to and use of information" [37]. Any attack aims to prevent or reduce the availability of information or services is considered as a denial of service attack.

Confidentiality is defined as "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information" [37]. So attacks that attempts to violate information secrecy are attacks against confidentiality.

Integrity is defined as "guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity."[37], so the attacks that attempts to alter or corrupt the data are attacks against information integrity.

4 Taxonomy Attack Vectors

Based on Fig. 1 a large number of MANETs attack vectors can be defined. Some of these vectors represent potential known attacks. An attack vector can constitute one or more attribute values from the same class.

The following is a list of some of taxonomy attack vectors that signify attacks commenced by external node/s and targets data confidentiality.

External → Singleton → Lack of Secure Boundaries → Protocol (RREQ) → Network (Confidentiality)
External → Collusion → Lack of Secure Boundaries → Protocol (RREQ, RREP) → Network (Confidentiality)
External → Singleton → Lack of (Secure Boundaries, central management) → Protocol (RREP) → Host (Confidentiality)
External → Collusion → Lack of Secure Boundaries → Protocol (RREP) → Host (Confidentiality)
External→ Singleton → Lack of Secure Boundaries, cooperativeness → Protocol (RTable) → Network (Confidentiality)
External→ Collusion → Lack of Secure Boundaries → Protocol (RREP, RTable) → Host (Confidentiality)
External→ Singleton → Lack of Secure Boundaries → Wireless Link (sniffing) → Network (Confidentiality)
External→ Collusion → Lack of Secure Boundaries → Host (IP) → Host (Confidentiality)

To show the taxonomy ability, we analyze the taxonomy vectors of some examples of well known MANETs attacks.

4.1 Description of Black Hole Attack

The blackhole attack involves malicious node or collusion of nodes fabricating the sequence number, hence pretending to have the shortest and freshest route to the destination. The attacker forges its destination sequence number, thus pretending to have the fresh enough route information to the destination.

More precisely, upon receiving the broadcasted Route Request message (RREQ), the attacker creates a Route Reply message (RREP) with a spoofed destination sequence number; a relatively high destination sequence number in order to be favored against others. Once the source node receives the reply from the attacker, it routes the data traffic through the attacker. Upon receiving the data packets, the attacker normally drops them and creates a 'black hole', as the attack name implies [38].

This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic.

From the above attack description, one possible taxonomy vector that represents a blackhole attack is:

Internal→ Singleton→ Lack of (Central Management) → Protocol (RREP) → Network (Availability)

A general vector that describes blackhole attack is:

Node (Internal/External) → No-of-Nodes (Singleton/Collusion) → Lack of (Secure boundaries, Central Management) → protocol (RREP/RREQ) → Host (Availability/ & Confidentiality/& Integrity)

Which read as; a blackhole attack can be launched by an internal or external single node or multiple of nodes, the attack make use of MANT's lack of secure boundaries and/or central management to exploit routing protocol control message RREP or RREQ to compromise victim's confidentiality and/or integrity and/or availability.

4.2 Description of Wormhole Attack

A wormhole attack [39] is one of the most sophisticated and severe attacks in MANETs. In this attack, a pair of colluding attackers record packets at one location and replay them at another location using a private high speed network.

From the above attack description, one possible taxonomy vector that represents a wormhole attack is:

Internal → Collusion → Lack of (Central Management) → Wireless Link (Bandwidth) → Host (Confidentiality)

A general vector that describes wormhole attack is:

Node (Internal/External) → No-of-Nodes (Singleton/Collusion) → Lack of (Central management, secure boundaries) → Wireless Link (Bandwidth) → Host (Availability/ & Conf./& Integrity)

Which read as; a wormhole attack can be launched by a collusion of internal or external nodes, the attack make use of MANT's lack of central management and or lack of secure boundaries to exploit a communication link to compromise victim's confidentiality, integrity or availability.

4.3 Description of Flooding Attack

In flooding attack [40], attacker exhausts the network resources, such as bandwidth and consumes a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. For example, in AODV protocol, a malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power, as well as network bandwidth will be consumed and could lead to denial-of-service.

From the above attack description, one possible taxonomy vector that represents a flooding attack is:

Internal → singleton → Lack of (Central Management) → Wireless Link (Bandwidth) → Network (Availability)

A general vector that describes flooding attack is:

Node (Internal/External) → No-of-Nodes (Singleton/Collusion) → Lack of (Central management, secure boundaries) → Exploited-Net-Res (Wireless Link (Bandwidth), Host (battery)) → Targeted (Network/Host (Availability))

Which read as; a flooding attack can be launched by a single/collusion of internal or external nodes, the attack make use of MANT's lack of central management and or lack of secure boundaries to exploit a communication link/ wireless host battery to compromise victim's availability.

4.4 Description of Rushing Attack

On-demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack. A malicious node which receives a Route Request packet (RREQ) from the source node floods the packet quickly throughout the network before other nodes receive the same original Route Request packet. Thus when nodes receives the legitimate Route Request packet they will assume those packets to be duplicates of the packet already received through the malicious node and hence discard those packets. Therefore, any route discovered by the source node would contain the malicious node as one of the intermediate nodes. Hence, the source node would not be able to find routes that do not include the adversary node.

From the above attack description, one possible taxonomy vector that represents the rushing attack is:

Internal → Singleton → Lack of (Central Management) → Protocol (RREQ) → Host (Availability/&Integrity/&Confidentiality)

A general vector that describes wormhole attack is:

Node (Internal/External) → No-of-Nodes (Singleton/Collusion) → Lack of (Central management, secure boundaries) → Protocol (RREQ) → Host (Availability/&Integrity/&Confidentiality)

Which read as; a rushing attack can be launched by a singleton or collusion of internal or external nodes, the attack make use of MANT's lack of central management and or lack of secure boundaries to exploit the RREQ message to compromise victim's confidentiality, integrity or availability**.**

5 Conclusions

The work in this paper is a novel work towards defining taxonomy to MANETs attacks. The taxonomy is an Attack Attributes-Based Taxonomy (AABT), that defines six classification criteria; attacking node legitimacy, number of attacking nodes, the utilized MANETs vulnerabilities, the exploited network resources, the targeted victim, and the compromised security service.

The proposed taxonomy is a start towards a well defined taxonomy of MANET attacks. In general it works well, and attacks are easily categorized, and it is expected to be an effective tool in analyzing MANETs attacks. However, as always for new developments, there is more to do for improvement and refinements.

Our future work is to define more precisely the values of each taxonomy attribute and to justify the completeness of the AABT through categorization of more actual attacks.

Competing Interests

Author has declared that no competing interests exist.

References

[1] Priyanka Goyal, Vinti Parmar, Rahul Rishi. MANET: Vulnerabilities, challenges, attacks, application. International Journal of Computational Engineering & Management. 2011;11.

[2] Sarkar SK, Basavaraju TG, Puttamadappa C. Ad hoc mobile wireless networks: Principles, protocols and applications, 1st ed.: Auerbach Publications; 2007.

[3] Perkins C. Ad Hoc Networks. Addison-Wesley; 2001.

[4] Zapata M. Secure Ad Hoc On-Demand Distance Vector (SAODV). Internet draft, draft-guerrero-manet-saodv-01.txt; 2002.

[5] Hu Y, Perrig A, Johnson D. Ariadne: A secure on-demand routing for Ad Hoc Networks. Proc. of MobiCom 2002, Atlanta; 2002.

[6] Simon Hansman, Ray Hunt. A taxonomy of network and computer attacks. Elsevier; 2004.

[7] Garcia Teodoro P, Sanchez L, Macia Fernansez G. Taxonomy and holistic detection of security attacks in MANETs. Security for multihop Wireless Networks, CRC press, Tayor & Francis Group; 2014.

[8] Abbott RP, Chin JS, Donnelley JE, Konigsford WL, Tokubo S, Webb DA. Security analysis and enhancements of computer operating systems. Technical Report NBSIR 76 1041, Institute for Computer Sciences and Technology, National Bureau of Standards; 1976.

[9] Bishop M. A taxonomy of (Unix) system and network vulnerabilities. Technical Report CSE-9510, Department of Computer Science, University of California at Davis; 1995.

[10] Howard JD. An analysis of security incidents on the internet 1989e1995. PhD thesis, Carnegie Mellon University; 1997.

[11] Lough DL. A taxonomy of computer attacks with applications to wireless networks. PhD thesis, Virginia Polytechnic Institute and State University; 2001.

[12] Yingbin liang. Information theory, IEEE transactions on. 2011;57(10): 6692–6702.

[13] Gagandeep, Aashima, Pawan Kumar. Analysis of different security attacks in MANETs on protocol stack a-review. International Journal of Engineering and Advanced Technology (IJEAT). 2012;1(5):2249 – 8958.

[14] Yian Huang, Wenke Lee. Attack analysis and detection for Ad Hoc routing protocols. In Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID 2004), Sophia Antipolis, France; 2004.

[15] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei. A survey on attacks and countermeasures in mobile Ad Hoc Networks. Springer; 2006.

[16] Aniruddha Bhattacharyya, Arnab Banerjee , Dipayan Bose. Different types of attacks in mobile ADHOC network: Prevention and mitigation techniques. URL: arxiv-web3.library.cornell.edu/pdf/1111.4090, 2011.

[17] Jawandhiya PM. A survey of mobile ad hoc networks attacks, International journal of Engineering Science and Technology. 2010;2(9):4063-4071.

[18] Cardenas A, Roosta T. Sastry S. Rethinking security properties, threat models, and the design space in sensor networks: A case study in SCADA System. AdHoc Network, 2009;7:1434-1447.

[19] Jain AK, Tokekar V. A classification of denial of service attacks in mobile ad hoc networks. International conference on computational intelligence and communication systems, Bali, Indonesia. 2011;256-260.

[20] Blazevic L, Buttyan L, Capkun S, Giordano S, Hubaux JP, Le Boudec JY. Self-organization in mobile Ad-Hoc networks: the Approach of Terminodes, IEEE Communications Magazine; 2001.

[21] Yongguang Zhang, Wenke Lee. Security in mobile Ad-Hoc networks, in book Ad Hoc Networks Technologies and Protocols (Chapter 9). Springer; 2005.

[22] Wu B, Chen J, Wu J, Cardei M. A survey on attacks and countermeasures in mobile Ad Hoc networks. Wireless/Mobile Network Security, Chapter 12. Springer; 2006.

[23] Hu YC, Perrig A, Johnson DB. Rushing attacks and defence in wireless Ad Hoc network routing protocols. In Proc. of the ACM Workshop on Wireless Security; 2003.

[24] Karlof C, Wagner D. Secure routing in wireless sensor networks: Attacks and countermeasures. Ad Hoc Networks. 2003;293-315.

[25] Bhalaji N, Shanmugam A. A trust based model to mitigate black hole attacks in DSR based manet. European Journal of Scientific Research. 2011;50(1):6-15.

[26] Latha Tamilselvan, Sankaranarayanan V. Prevention of black hole attack in MANET. The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 0-7695-2842-2/07; 2007.

[27] Hu YC, Perrig A, Johnson DB. Packet leashes: A defence against wormhole attacks in wireless Ad Hoc networks. In Proc. of INFOCOM; 2003.

[28] Awerbuch B, Holmer D, Nita-Rotaru C, Rubens H. An on-demand secure routing protocol resilient to byzantine failures. Proceedings of the ACM Workshop on Wireless Security. 2002;21-30.

[29] Chang Wu Yu, Tung-Kuang Wu, Rei Heng Cheng, Shun Chao Chang. A distributed and cooperative black hole node detection and Elimination Mechanism for Ad Hoc Networks", PAKDD 2007 Workshops, LNAI 4819. 2007;538–549.

[30] Santhosh Krishna BV, Vallikannu AL. Detecting malicious nodes for secure routing in MANETS using reputation based mechanism. International Journal of Scientific & Engineering Research. ISSN 2229-5518. 2010;1(3).

[31] Priyanka Goyal, Vinti Parmar, Rahul Rishi. MANET: Vulnerabilities, challenges, attacks, application. IJCEM International Journal of Computational Engineering & Management. 2011;11.

[32] Brickell E, Feigenbaum J, Maher D. DIMACS workshop on trust management in networks, South Plainfield, NJ; 1996.

[33] Chlamtac I, Conti M, Liu J. Mobile ad hoc networking: Imperatives and challenges. Ad Hoc Networks Journal Elsevier. 2003;1(1):13–64.

[34] Lauer GS. Routing in communication networks, Englewood Cliffs, NJ: Prentice Hall; 1995.

[35] Zhenzhen Y, Yingbo H. Stability of wireless relays in mobile ad hoc networks, in Proceedings of Acoustics, Speech, and Signal Processing, (ICASSP '05). IEEE International Conference on. 2005;3.

[36] Buttyan L, Hubaux JP. Stimulating cooperation in self- organizing mobile ad hoc networks, ACM/Kluwer (MO- NET), Special Issue on Mobile Ad Hoc Networks. 2003;8(5).

[37] Standards for Security Categorization of Federal Information and Information Systems. Federal Information Processing Standards Publication; 2004.

[38] Sun B, Guan Y, Chen J, Pooch UW. Detecting black-hole attack in mobile Ad Hoc networks. Paper presented at the 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom; 2003.

[39] Hu YC, Perrig A, Johnson D. Wormhole attacks in wireless networks. IEEE JSAC. 2006;24(2).

[40] Pradip M. Jawandhiya, et al. A survey of mobile Ad Hoc network attacks. International Journal of Engineering Science and Technology. 2010;2(9): 4063-4071.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
www.sciencedomain.org/review-history.php?iid=726&id=6&aid=6734