Universal Journal of Communications and Network 6(2): 7-17, 2018 http://www.hrpub.org
DOI: 10.13189/ujcn.2018.060201

Security Threats and Solutions in Mobile Ad Hoc Networks; A Review

Mutuma Ichaba

Institute of Open and Distance Learning, Africa Nazarene University, Kenya

Abstract Compared to wired-infrastructure dependent networks, Mobile Ad Hoc Networks (MANETs) are more vulnerable to attacks. Because of their dynamic topology and the absence of centralized network administration, MANETs face more security threats than centralized networks. Initial literature review on MANETs' security issues indicates that while there have been attempts to identify security threats and solutions on MANETs, comprehensive reviews are very little or lacking. In an attempt to address this gap, this article offers an up-to-date literature on security issues and solutions in MANETs. By limiting the review to 21st Century research on this topic, this review paper is able to offer a comprehensive presentation of the issues concerning security in MANETs.

Keywords Mobile Ad Hoc Networks **(**MANETs), Security, Threats, Solutions, Routing Protocols

1. Introduction

In present-day society mobile devices (e.g laptops and cellphones) are increasingly being integrated to daily activities. This makes them an integral, inseparable and critical part of life in contemporary society. Literally, mobile devices are found virtually anywhere there is human life. For this reason, ever more, these mobile devices are required to interconnect to pass messages along between individuals and groups, thus enabling effective communication [7]. Habitually, these devices interconnect to enable responses to the demands of specific scenarios. Such case-specific demands include emergency situations—rescue operations for example, and in military combat zones. "With the various routing protocols, resource limitations, and different communications mediums utilized by these networks, security is typically not at the forefront of their design" [7].

Making sense of the latent threats to ad hoc networks' security, it is vital to understand the meaning of the terms "ad hoc" [8]. "Ad hoc" is a Latin word for "this specific purpose". As the terms indicate, the core nature of the purpose of ad hoc networks is the notion that they are formed on-demand basis. That is, ad hoc networks are formed to respond to scenarios where traditional networks are either unavailable, damaged or inapplicable. Additionally, the main qualities of ad hoc networks are that they can be spontaneous, impermanent, purpose-built, distributed, and autonomous [8].

Besides, ad hoc networks are characteristically vastly tailored based on the need of a situation. Every scenario calls for its uniquely customized ad hoc network [9], [10]. Expectedly, ad hoc networks follow the administrative and security processes found in conventional wired networks. Yet, whereas discrete deployments of ad hoc networks can differ significantly, they share certain common characteristics. In [7], such traits listed include "lack of central control, limited resources, mobility, dynamic topologies, wireless connectivity, and/or custom routing protocols". Unsurprisingly, each of these characteristics bring in unique security issues. A case in point; decentralization in ad hoc networks means an absence of centralized administration thus lacking a unified security regulation point and mechanism. Consequently, wireless networks in general and mobile ad hoc networks in particular, are prone to external threats such as signal interference and jamming. Also, because mobile ad hoc networks experience limited resources, they may not accommodate non-customized conventional routing protocols. Customization, occasionally, may corrupt the effectiveness of existing security cautions.

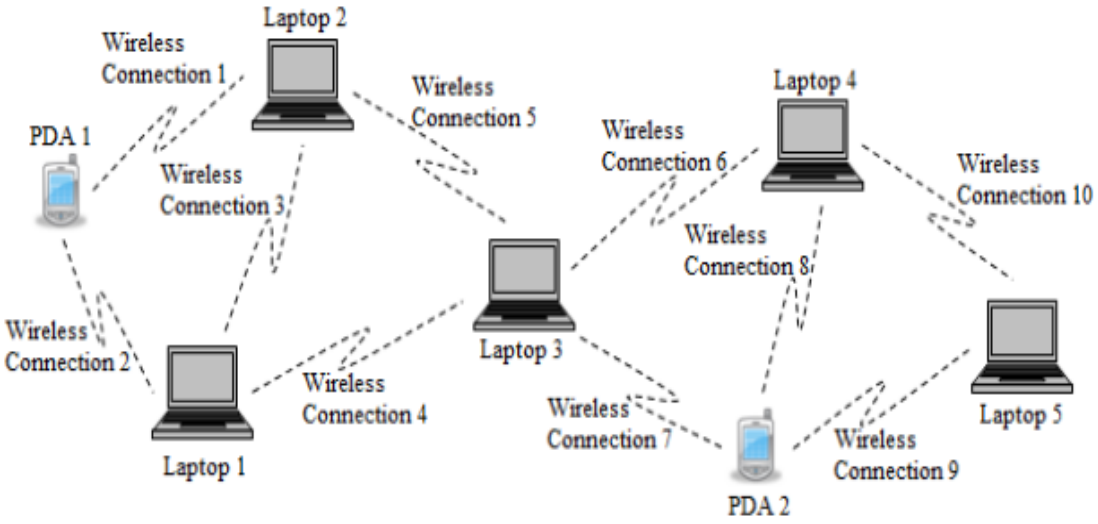

Figure 1. An Example of Mobile Ad Hoc Network [2]

Mobile Ad hoc Networks (MANETs) are made up of self-configuring mobile nodes linked through wireless connections [1]. MANETs' nodes that are adjacent to each other may transmit information between them, while they depend on immediate nodes to pass information to other nodes in the network. A mobile node may serve either as a sender, receiver or a router. Mobile Ad-hoc Networks (MANETs) are described by their ability to multi-hop, self-configure, and their fluidity as nodes join and leave the network. MANETs are made up of cluster(s) of mobile devices whose terminals are connected wirelessly. Mobile terminals serve both as the receiver and the transmitter of information—router and host. MANETs require no infrastructure while at the same time being very dynamic. Because of this need-based trait of the MANETs, they have been highly applicable in the areas or situations that require momentary responses.

Because nodes in MANETs do not depend on fixed infrastructure, approach to their security issues is always different from their wired counterparts [3]. The security challenges availed by nodes in MANETs are quite different from the security issues that face infrastructure-dependent nodes. Moreover, because MANETs are case-specific—designed to respond to the demands of particular unique scenarios, solutions to their security are different from the infrastructure-dependent networks. Due to the autonomy of nodes to either join or leave the network, traditional security solutions of networks can be inapplicable. Therefore, it is wise to use scenario-based security responses while utilizing MANETs.

Wireless transmission of data packets in MANETs exposes the signal to possible intrusion from malicious attackers [4]. Unlike in the wired networks, it is easier to tap into MANETs' signals. As noted in [5], wireless propagation of data packets introduces vulnerability in the network because generally, their data shielding and security are relatively poor. Consequently, very so often, MANETs are prone to signal "interference, jamming, eavesdropping and distortion" [4]. Accordingly, routing protocols in MANETs are, in most cases, designed to handle such this vulnerability. High mobility of nodes in MANETs complicates security efforts compared to wired networks [6]. By taking advantage of the security gaps created by moving nodes, attackers may break either into the whole network or concoct partial attack. Due to so many characteristics of MANETs—high mobility, dynamism, and autonomy, there are numerous security issues and threats that require attention.

Mobile ad hoc networks use their nodes as both routers/transmitters and receivers. Because of this dual-purpose status of nodes, every mobile device in a network is very critical to the security of data transmission [14]. Consequently, a compromised node may become contagious to the rest of devices. While designing a mobile ad hoc network, it is vital to always consider this mutual overreliance among the neighboring nodes. This is so because all nodes in ad hoc networks maintain topological information of the neighboring nodes. Infection or an attack in one node can spread rapidly if not contained properly.

Connectivity in MANET, typically occurs at the link-layer protocol and network-layer protocol [15], [16]. A single-hop connection takes place at the link-layer protocol, while multiple-hop connection occurs at network-layer. Resultantly, to attain maximum security in data packets transmission, it is critical to implement safety measures at both layers-link-layer and network-layer [15]. At the link-layer security installation, the one-hop connectivity amid two end-to-end nodes that are within each other's communication range through secure protocols, such like the IEEE 802.11 WEP protocol [17] or the added lately anticipated 802.11i/WPA protocol [18] are protected. Secure multi-hop propagation and delivery of data packets is executed by the network-layer.

Network-layer guarantees effective and reliable transmission of data signals in line with the security stipulations embedded in the routing protocols. Hence, security issues are defined by their points of attacks. That is, a security issue in MANETs can either be labelled as a routing protocol question or general network threats.

Links of wireless nodes in mobile ad hoc networks are unreliable for safe and steady connectivity [19]. As the nodes leave and join the network, topological information changes. The change in topological information in nodes' tables can avail weak points for attacks by malicious intruders. Additionally, the unreliability of ad hoc mobile nodes can result from inadequate energy supplies to the devices [21]. Accordingly, limited power supplies to the devices and the consistent movements of nodes around networks, negatively affects the overall security and the communication. Study [20] observers that in some instances, mobile ad hoc nodes have inadequate integration and implementation of security structures.

MANETs attacks and threats can originate either externally or internally [23]. Internal attacks are the security threats that emanate from the users and nodes/devices within the network. Familiarity with of the network is very useful in the formulation of internal attacks. Users of a network may, sometimes possess vital information necessary in the disruption of messages, deletion of records or even denial of network services. Normally, internal attacks are directed to the network links and security interfaces [22]. External attacks, on the other hand, involves execution threats from outside the network. These attacks are divided into two. That is, active and passive attacks. Comparatively, active attacks cause more damage than passive attacks.

2. Literature Review Methodology

In an effort to generate the most up-to-date literature on MANETs' security threats, issues and solutions, Google search engine was used to access articles from various websites and databases. Firstly, research articles generated by general search on Google were reviewed based on key terms such as "mobile ad hoc", "security", "threats" and "solutions". Moreover, research articles were further selected based on their appearance in websites such as ResearchGate, Springer, Elsevier, Google Scholar or IEEE. The key terms used on Google search were designed to capture the categories of words and phrases such as Mobile Ad Hoc Networks (MANETs), security, threats, and solutions– mobile ad hoc*MANETs OR ad hoc network(s) OR Wireless Ad hoc network(s)* AND security* AND threats OR issues* AND solutions.

To ensure a balanced representation of studies, the following criteria was used:

a). Every security threat was picked from a single study
b). Every solution to the MANETs security threat was selected from a single study
c). Routing Protocols and MANETs characteristics were selected randomly from various studies

This review paper is divided into five sections. That is, the introduction, methodology, related research, categories of security threats, security measures/solutions to the threats, conclusion and further research recommendations.

3. Related Research

A number of studies have been carried out on security challenges and solutions in mobile ad hoc networks MANETs. MANETs attacks may take place in two major ways. That is, either passively or actively. In passive attack, the data under transmission is not affected. Rather, passive attack pretends to be part of the data, but with the sole motive of collecting important information [39]. A passive attack may be seen as planting an evil spy within a group of good guys with intention of stealing information. There is no disruption of routing while passive attack occurs. In an active attack, nonetheless, the transmission of data is interrupted. Compared to the passive attack, an active attack is more severe because the normal transmission of data between nodes is negatively affected, write Kaur and Sukhman [39]. Either of the types of attacks can emanate internally or externally.

Because MANETs depend on nodes for self-reorganization, their network systems are more vulnerable to attacks than the wired networks. For this reason, securing MANETs can be a daunting task. But there are security objectives that must be pursued in MANETs to guarantee some safety for the users. Confidentiality should be always considered. Only the authorized devices and users are allowed to access the network to protect privacy and secrecy [40]. Every node requires the capability to validate the ingenuity of the peer node and user. Valid network users and nodes need validation credentials to access the network. Authentication prevents imitators from accessing the network illegitimately.

Other studies such as the one conducted by Zhou and Haas [42], suggest the deployment of edge cryptography to guarantee network security for providing security. Hubaux et al. [43] outlines procedures for enabling individual nodes in a network to authenticate the security of a fellow node thus issuing security certificates. Moreover, Kong, et al. [8] propose a MANET routing protocol that bases its security on surreptitious sharing of information under transmission within the network and the possible security threats. Additionally, Yi et al. [44] offer a general model for securing data transmission and connectivity in a MANET.

Also, Deng et al. [45] provides a possible response to the threats of posed by "black hole" attack, Sanzgiri et al. [46]

suggests for a secure MANET routing protocol dubbed ARAN. This protocol uses certifications of nodes to warrant security in a network. Certifications, according to Sanzgiri et al. [46], has the potential to overwhelm any security threat directed to MANET network. Supplementary works of Yang et al. [47] conducts a comprehensive presentation and discussions on security issues and threats affecting multihopping in MANETs. In the same review [47], issues relating to the design of security and contemporary status of security in the transmission of data packets, are highlighted.

Due to their vulnerability, researchers have developed numerous ways of fighting insecurity in MANETs. For instance, Intrusion Detection is a response scheme for detecting threats beforehand. Intrusion Detection put forth both "distributed and cooperative model," designed for sensing and identifying attacks [41]. Sheikhl et al. [41] observe that in the Intrusion Detection all nodes in a network are called to action. Once a node identifies a threat independently, it broadcasts a warning to the rest of the nodes. But at times, as a result of power limitation of the nodes, the dissemination of the warning may not be successful. Such incidents require cluster-driven Instruction Detection. Cluster-driven Intrusion Detection is designed in such a way that the network is divided into subgroups (clusters). Clusters enable the member nodes to disseminate attack warnings to the companion nodes. Intrusion detection role is assigned to a single node that serves as the watchman for others. Every time an attack is detected, the responsible node is expected to alert the rest of the nodes in the cluster. All nodes assigned to a cluster are served by one radio range.

Some other MANETs attacks include the Wormhole. Packet leash is an attack response to the wormhole, note Sheikhl et al. [41]. Wormhole intercepts information under transmission in pretense of being a genuine receiver. The information intercepted is tunneled to another wormhole attacker. The intercepted information is corrupted by the wormhole and resent to the genuine receiver. Although the message is disguised as valid, it carries hidden scripts designed to steal information or disable the line of transmission. Response to wormhole attack includes adding extra information to a packet to regulate the maximum distance of transmission—this called packet leashing. Packet leashing can be either geographically bound or temporal bound. Geographically bound packet leashing uses the distance to regulate the transmission of a packet, while temporal bound packet leashing deploys the maximum time of packet transmission.

4. Types of Security Threats in MANETs

Because MANETs connections and the transfer of data packets rely on clusters of nodes or mobile devices that form, in most cases, short-lived hence temporary networks, the need for a central administration is eliminated. For this reason—the lack of central administration, the interconnection of mobile nodes must be based on absolute trust. Moreover, due to dynamic nature of MANETs and thereof rapid change of topological information, comparatively, they are susceptible to internal attacks.

Attacks in MANETs can be categorized based on network layers [24]—see figure 2.

Flooding is an attack in MANETs that disrupts the normal functioning of a network by hijacking its resources. For example, a malicious node designed to attack can overuse the bandwidth & power to interpose and establish distress in the performance of a network [25]. The Black Hole Attack occurs when a malicious node distributes a wrong signal to the rest of the network nodes. Such a signal message may indicate to the rest of the nodes that the infected node is the best of the available routes around the network. What follows is an automatic forwarding of the topological information of the network to the infected node [26]. Link Spoofing is a network layer attack that occurs when a malicious node broadcasts bogus link information to the rest of the nodes. Because the transmitted phony link messages are erroneous, the entire operations of the network are disrupted [27], [28]. Network Partitioning attack divides the network into sub-networks to introduce unnecessary heterogeneity in packet data and topological information transmission [29]. The unnecessary heterogeneity within a MANET network ensures an absence of reliable routes, thus disabling effective transmission within the network.

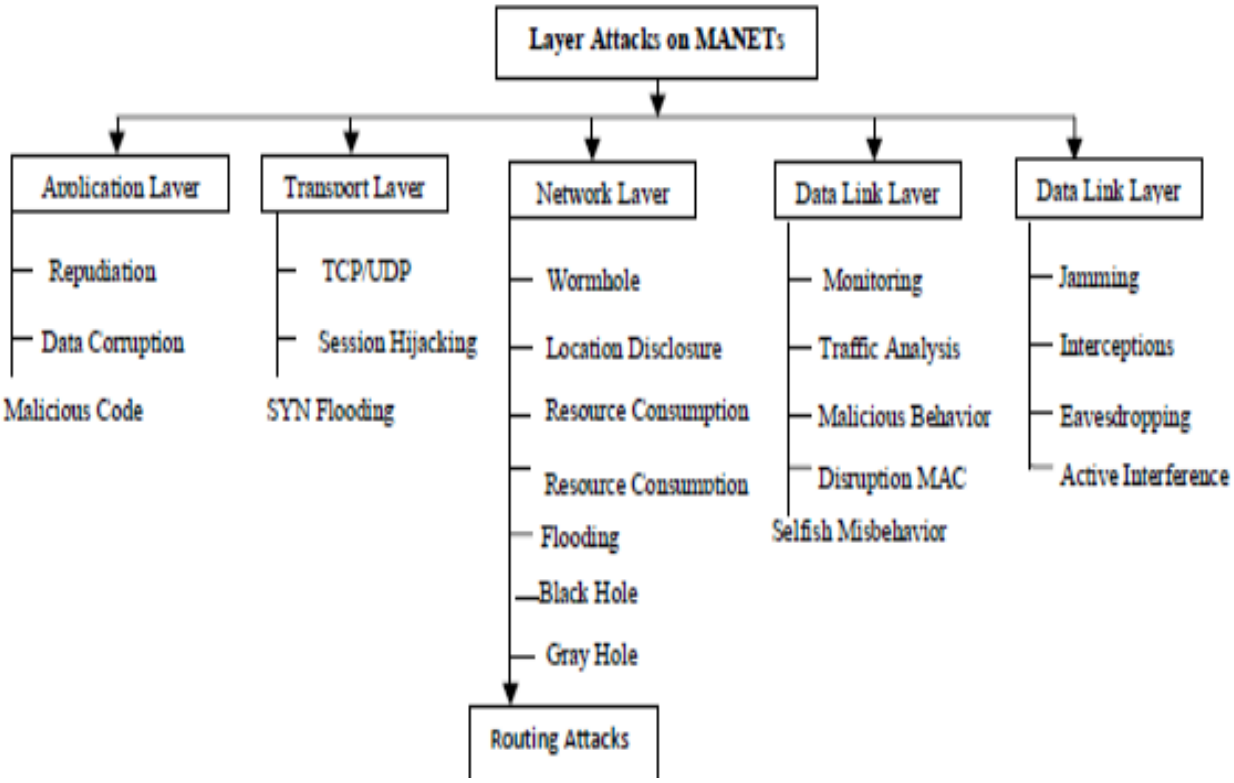

Figure 2. Attacks in various layers of MANET [24]

Other network layer attacks in MANETs include Selfishness [30]. In this attack, an infected node act malevolently and uncooperatively. Since MANETs nodes are supposed to act both as router/receiver and transmitter, selfish nodes can decide to not to execute either of the roles. By assuming dormancy, a node thus introduces a link breakage in the network. In Sleep Deprivation attack, a node within a MANET network is forced to overuse its power supply [31]. Overusing of power supply—typically, the batteries, results into shorted overall usability of the node and sometimes reduced service life. Denial of Service (DoS) occurs when an infected node blocks the reception and the transmission of data packets and other network topology information among the other nodes.

In paper [32], Grey Hole attack introduces "red herrings" in data packet transmission. Grey Hole attack arises when an attacker approves malicious routes as valid. Upon endorsing an insecure route, data is redirected to an attacker, thus introducing difficulties in the general working of the network. When an attacker receives the data packets, they are immediately, dropped, corrupted or destroyed. Jellyfish attack creates unnecessary inconveniences and disruptions within a MANET network [33]. For instance, Jellyfish attack may contaminate a single node or several nodes to create, however deliberately, the delay of packet transmission time.

Delayed transmission time, on the other hand, brings in an overall reduction in network's performance. Resource Consumption attack comes about as a result of an infected node purposely infiltrates the resources of other nodes such batteries and bandwidths [34]. Another MANETs networks attack is Detour [35]. In Detour attacks, malicious nodes ensure diversion of data packets transmission routes. Detour attacks corrupts the original routes information stored in respective network nodes, hence introducing confusion in broadcast within the network.

Apart from categorizing MANETs attacks based on network layers, security threats can be grouped based on source, behavior and nodes [36].

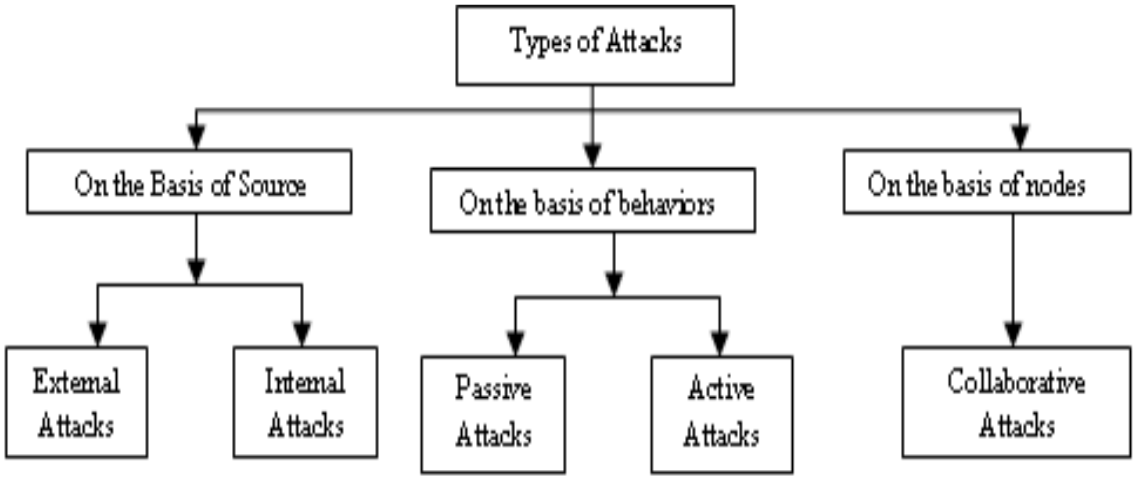

Figure 3. Categorization of Attacks in MANETs based on source, behavior and nodes [36]

Passive attacks are designed to snip information under transmission in a network [49]. In this category of attacks, intrusion does not cause any detectable disturbance within the network. While sniffing of information takes place, noticeable activities such as the dropping of data packets or the introduction of false packets are avoided. Literally, passive attacks assume the part of the network while maintaining a keen watch over the information in transmission [50]. Because of their malicious inert participation in a network, these attacks easily intrude the confidentiality constraints of data. Passive attacks are very hard to detect because they avoid instigation of any malevolent operation that may interrupt the ordinary running of the network. Cases of such types of attacks include traffic analysis, traffic monitoring and eavesdropping [38].

On other hand, active attacks are comparatively disruptive [51]. Active malicious nodes alter the network traffic and the overall transmission by causing congestion, propagation of false and corrupted routing information. As a result of their active nature of attacks, their detection and thereof prevention are achievable relatively easily. Examples of passive attacks comprise modification attack, impersonation, fabrication and message replay [52,53,54].

MANETs attacks can also be grouped based on their location relative to the network under attack. This criterion classifies attacks either as internal or external. External Attacks are initiated by unlicensed malicious nodes that are not part of the network [56]. External attackers may flood false packets in the network and sometimes imitates authentic nodes [55]. External malicious nodes mainly, intents to cause cramming or interruption of ordinary network working. Oppositely, internal attacks are instigated by the authentic nodes in a network. Internal attacks aim at either hijacking authorized nodes and in turn use the as proxy attackers or arbitrary selfish and greedy seizing of resources from other network nodes—battery power, processing power, and bandwidth. Greedy seizing of network resources may result as a designed and intentional exploitation of member nodes [57].

5. Solutions to MANETs' Security Threats

There are several techniques suggested to thwart security threats in MANETs. For example, [39] observes that, essentially, there are two methods to securing a MANET. That is, the proactive and reactive approaches. In proactive approaches, cryptography is the main method applied—altering signals under transmission so that they are not easily decrypted. Proactive methods are actively in action during the operations of a network. Oppositely, reactive techniques are designed to respond upon detection of a security threats.

Until a threat is detected, reactive safety measures stay dormant within the network. Each of these tactics has their qualities, strengths and weaknesses. Consequently, every security measure is suited and appropriate at responding to various security threats. Majority of secure routing protocols assume and implement the proactive methods to safeguard message signals under transmission [40,41]. On the other hand, a few routing protocols deploy reactive safety methods while conducting data packet forwarding.

Other studies such as [34], identified the security threats in each of the network layers and equivalent countermeasures. The subsequent table summarizes latent "security attacks and the actions that can be taken to prevent the attacks".

Because security and threats in MANETs are not as well defined as they are in infrastructure-dependent networks, it is critical that the line of defense proposed be as comprehensive as possible. As such, any security solution for MANET must incorporate both the proactive and reactive measures while and combining prevention, detection, and reaction [47]. Prevention element prevents attacks by expressively augmenting the challenge of disrupting the network.

Table 1. Security Threats and possible responses in MANETs [34]

Layers	Attacks	Solutions
Application layer	Lack of cooperation attacks, Malicious code attacks (virus, worms, spywares, Trojan horses) etc.	Cooperation enforcement (Nuglets, Confidant, CORE) mechanisms, Firewalls, IDS etc.
Transport layer	Session hijacking attack, SYN flooding attack, TCP ACK storm attack etc.	Authentication and securing end-to-end or point-to-point communication, use of public cryptography (SSL, TLS, SET, PCT) etc.
Network layer	Routing protocol attacks (e.g. DSR, AODV etc.), cache poisoning, table overflow attacks, Wormhole, blackhole, Byzantine, flooding, resource consumption, impersonation, location disclosure attacks etc.	Source authentication and message integrity mechanisms to prevent routing message modification, Securing routing protocols (e.g. IPSec, ESP, SAR, ARAN) to overcome blackhole, impersonation attacks, packet leashes, SECTOR mechanism for wormhole attack etc.
Data link layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness etc.	No effective mechanism to prevent traffic analysis and monitoring, secure link layer protocol like LLSP, using WPA etc.
Physical layer	Jamming, interceptions, eavesdropping	Using Spread spectrum mechanisms e.g. FHSS, DSSS etc.

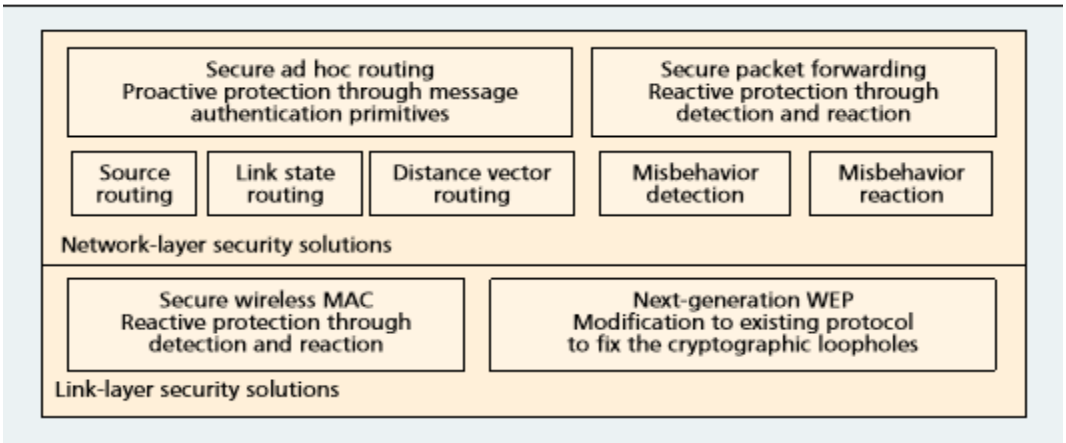

Figure 4. The components in the multifence security solution [47]

Consequently, the detection and reaction mechanisms determine malicious interferences and respond accordingly. These mechanisms are critical because they enable a network evade insistent hostile attacks— they are essential for other security measures to operate in diminished security threats. The detection constituent senses attacks by identifying irregular activities as revealed by malevolent nodes. Such abnormal activity is sensed either "in an end-to-end manner, or by the neighboring nodes through overhearing the channel and reaching collaborative consensus" [47]. Upon identifying a threat node, the reaction element corrects the routing and forwarding procedures. For example, such an activity may involve either avoiding the routes that go through the identifies threat node or mutually excluding the node from the network.

Study [58] attempts to highlight various security issues in comprehensive manner. Koul and Sharma [58], upon extensive review of literature on MANETs security and their solutions, created a summary table—see table 2.

Table 2. Security Mechanisms used to protect MANETs [58]

Secure methods Explored	Approaches followed	Security methods used
Watchdog & Pathrater	Reputation based	Nodes are watched promiscuously by Watchdog and a buffer of recently sent packets is maintained to compare with each overheard packet. If a packet remained for longer than timeout, increments a failure tally for the node responsible and if tally exceeds a threshold, the node is declared to be misbehaving and the source is notified.
Watchdog & Pathrater	Reputation based	Nodes are watched promiscuously by Watchdog and a buffer of recently sent packets is maintained to compare with each overheard packet. If a packet remained for longer than timeout, increments a failure tally for the node responsible and if tally exceeds a threshold, the node is declared to be misbehaving and the source is notified.
SAR	Hybrid approach	Keys generation using different trust levels, use digital signatures.
ARAN	Asymmetric cryptography	Trusted certificate server is used to generate and distribute cryptographic certificates. Digital signatures are also used to validate them. Each node knows a priori the public key of the trusted certification authority and obtains exactly one certificate after securely verifying its identity to the server.
ARIADNE	Symmetric cryptography	Clock synchronization, a shared secret between each pair of nodes, an authentic TESLA key for each node in the network is distributed by KDA, uses digital signature to sign routing messages and an authentic route discovery chain element for each node.
Detecting forged routing messages in ad hoc networks	Intrusion detection system	Used where cryptographic based solutions don't work. Alert messages are flooded on detecting a suspect. Suspect is declared as an intruder when other nodes also raise alerts. N is the no. of nodes that can raise alerts. N is taken as 2.
Detection of the node-capture attack in mobile wireless sensor networks	Observation based	Based on tracking of other nodes and re-meet of two nodes within the time set. If they don't meet or time-out expires, an alarm is flooded to announce that node's absence. (MIT) is taken as parameter to suppress fake alarms and to avoid false positives.
SRAC	Hybrid approach & trust based	Each node has an initial pair of public/private keys embedded into each node at the initialization phase or created by a self-organized public key management system. Based on evaluating redundant routing messages received at the target by their TQI (trustworthiness-QoS index) values.
High Performance Firewalls in MANETs	Source prefix filtering constraints	Source prefix filtering constraints are implemented in the route reply packets of the underlying routing protocol used which is used to control route propagation and packet forwarding.
FrAODV	Trust based	IP and MAC addresses are used to identify friend. Friend list is created in the initialization phase or distributed offline. Routing messages are only received by friend nodes by evaluating their friendship values.
TSR	Double layer approach	Observes contention window abnormalities in transport layer and react accordingly in network layer. Control packets are authenticated via security mechanisms [1] [2].
E-ARAN	Reputation based	Based on observation of neighbor nodes, a faulty list is maintained to store all those faulty nodes whose threshold falls below -40 (already preset) and each node stores a route ranker table to choose the high reputed route. Selfish nodes if drops the packets then their reputation go down and the route established by them may not be selected.

Further similar reviews can be found in articles [59], [60], [61], [62], [63], [64], [65]

6. Aspects of Security in MANETs

Paper [11] notes that one of the network aspects that is affected by malicious attacks include the denial of network availability. Availability in mobile ad hoc networking connotes the ability of the network's nodes to steadily execute their tasks without unplanned or unnecessary interruptions [12]. The Denial of Service (DoS) is one of the attacks that interrupts and corrupts accessibility of a network. Network integrity is another aspect that can be attacked in a mobile ad hoc network. Network integrity ensures that the identity of data packets under propagation are maintained [13].

Data integrity security can be compromised in two main ways [34]. That is, through malicious altering and accidental altering. In malicious attacks on data integrity, a data packet under transmission may be deleted, replaced or corrupted. However, if a data packets or its contents is either lost or altered as a result of natural network malfunction, the occurrence is dubbed accidental altering. Confidentiality of messages is another piece that can be compromised by malicious intruders. Attacks on data confidentiality occurs when unauthorized persons or agents access messages that otherwise they are not allowed to.

Malicious attacks can also compromise the authenticity of data. Authenticity of data is breached when impersonators gain access to the data. To avoid these threats and attacks, it is vital that appropriate authentication procedures be embedded in the routing protocols of mobile ad hoc networks. Persons or agents accessing a network must always prove their identities for authorization. Potential user entities for the network require standardized and secured credentials. Similarly, encryption of access credentials is paramount in maintaining anonymity and

thereof privacy [42].

7. Conclusions and Further Research Recommendations

From this review article, it is clear that there are plenty of studies that attempt to highlight security issues and their solutions in MANETs. However, virtually all of them fail to provide a comprehensive review in regard to security issues and their solutions in MANETs—they lack features such as exhaustive categorizations of security threats. In response to this deficiency in literature, this article tries to present a comprehensive review of literature on MANETs' security issues—mainly threat and solutions. It is noted, nonetheless, that the society faces constant advances in technology, thus augmenting new innovations. As such, it is critical that researchers continue to review new additions to the existing studies. The area of MANETs is only likely to grow. For this reason, continuous compiling of these developments is critical to its knowledge. Future research can include examinations and explorations of areas such the future of MANETs and the impact of MANETs to the education and agricultural sectors.

REFERENCES

[1] A. Rai, V. Srivastava and R. Bhatia, "Wormhole Attack Detection in Mobile Ad Hoc Networks", *International Journal of Engineering and Innovative Technology (IJEIT)*, vol. 2, no. 2, 2012.

[2] R. Almaharmah, "Multi-Aware Cluster Head Maintenance for Mobile Ad Hoc Networks with Wireless Power Transfer Capabilities", Ph.D, Universität Duisburg-Essen, 2016.

[3] V. Kärpijoki, "Security in Ad Hoc Networks", in *Tik-110.501 Seminar on Network Security*, Helsinki University of Technology, 2000.

[4] C. Nayak and M. Pradhan, "Security Issues in the Ad-Hoc Network Environment", *International Journal of Scientific Engineering and Research (IJSER)*, vol. 1, no. 1, 2013.

[5] S. Yi, P. Naldurg and R. Kravets, "Security-aware ad hoc routing for wireless networks", *Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing - MobiHoc '01*, 2001.

[6] S. Sarika, A. Pravin, A. Vijayakumar and K. Selvamani, "Security Issues in Mobile Ad Hoc Networks", *Procedia Computer Science*, vol. 92, pp. 329-335, 2016.

[7] R. Derveloy, "Security Issues of Ad Hoc Networks", *CPSC-5620 SPRING 2012*, 2012.

[8] "ad hoc | Origin and meaning of ad hoc by Online Etymology Dictionary", *Etymonline.com*. [Online]. Available: https://www.etymonline.com/word/ad%20hoc. [Accessed: 29- Nov- 2018].

[9] P. Yau and C. Mitchell, "Security Vulnerabilities in Ad Hoc Networks ∗", 2003.

[10] "Definition of AD HOC", *Merriam-webster.com*. [Online]. Available: https://www.merriam-webster.com/dictionary/ad%20hoc. [Accessed: 29- Nov- 2018].

[11] Z. Ishrat, "Security issues, challenges & solutions in MANET", *International Journal of Computer Science & Technology*, vol. 2, no. 4, pp. 108-112, 2011.

[12] K. Nahrstedt, W. He and Y. Huang, "Security in Wireless Ad Hoc Networks", *Computer Communications and Networks*, pp. 391-425, 2009.

[13] D. Finestone, "What is Data Integrity and 12 Ways to Reduce Data Integrity Risk", *GlobalVision Blog*. [Online]. Available: https://www.globalvisioninc.com/blog/12-ways-to-reduce-data-integrity-risk/. [Accessed: 29- Nov- 2018].

[14] M. Kumar, N. Geethanjali and N. Babu, "Security issues in Mobile Ad-Hoc Networks", *International Journal of Engineering Inventions*, vol. 2, no. 11, pp. 48-53, 2013.

[15] B. He, J. Hägglund and Q. Gu, "Security in Ad Hoc Network."

[16] H. Zhao, "Security for Ad Hoc Networks", Columbia University.

[17] IEEE Std. 802.11, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 1997.

[18] IEEE Std. 802.11i/D30, "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security," 2002.

[19] W. Li and A. Joshi, "Security Issues in Mobile Ad Hoc Networks - A Survey."

[20] A. Mishra and K. Nadkarni, *The handbook of ad hoc wireless networks*. 2003.

[21] I. Kaur, N. Kaur, Tanisha, Gurmeen and Deepi, "Challenges and Issues in Adhoc Network", *International Journal of Computer Science And Technology*, vol. 7, no. 4, 2016.

[22] P. Sharma, "A Review: Security Issues in Mobile Ad Hoc Network", *International Journal of Computer Science and Mobile Computing*, vol. 3, no. 5, pp. 365-370, 2014.

[23] U. Karthikeyan and Rajani, "Security Issues Pertaining to Ad-Hoc Networks", 2012.

[24] U. Singh, K. Phuleria, S. Sharma and D. Goswami, "An analysis of Security Attacks found in Mobile Ad-hoc Network", *International Journal of Advanced Research in Computer Science*, vol. 5, no. 5, pp. 34-39, 2014.

[25] M. Hussain and M. Hasan, "Collective Study On Security Threats In MANET", *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH*, vol. 6, no. 01, pp. 32-37, 2017.

[26] S. Kumar, M. Goyal, D. Goyal and R. Poonia, "Routing Protocols and Security Issues in MANET", in *2017 International Conference on Infocom Technologies and Unmanned Systems (ICTUS'2017)*, ADET, Amity University Dubai, UAE, 2017.

[27] A. Yadav and K. Singh, "Evaluation of Security Threats and Solutions in MANET'S", *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 6, no. 2, pp. 537-542, 2016.

[28] P. Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 1, no. 5, pp. 269-275, 2012.

[29] V. Kärpijoki, "Security in Ad Hoc Networks", in *Tik-110.501 Seminar on Network Security*, 2000.

[30] S. Jain, "Security Threats in Manets: A Review", *International Journal on Information Theory*, vol. 3, no. 2, pp. 37-50, 2014.

[31] A. Sandoval Orozco, J. García Matesanz, L. García Villalba, J. Márquez Díaz and T. Kim, "Security Issues in Mobile Ad Hoc Networks", *International Journal of Distributed Sensor Networks*, vol. 8, no. 11, p. 818054, 2012.

[32] P. Parwekar and S. Arora, "Security Issues and Its Counter Measures in Mobile Ad Hoc Networks", *ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India- Vol I*, pp. 301-309, 2014.

[33] Priti and P. Sharma, "A Review: Security Issues in Mobile Ad Hoc Network", *International Journal of Computer Science and Mobile Computing*, vol. 3, no. 5, pp. 365-370, 2014.

[34] K. Biswas and L. Ali, "Security Threats in Mobile Ad Hoc Network", Master's, Blekinge Institute of Technology, 2007.

[35] A. Tehlanl and D. Sharma, "A Study on Different Security Threats in Mobile Ad-hoc Network", *International Journal of Information and Computation Technology.*, vol. 4, no. 1, pp. 1-10, 2014.

[36] S. Aluvala, K. Sekhar and D. Vodnala, "Analysis of Security Threats and Issues in MANETs", *International Journal On Advanced Computer Theory And Engineering (IJACTE)*, vol. 4, no. 5, 2015.

[37] S. Pareek, A. Gautam and R. Dey, "Different Type Network Security Threats and Solutions, A Review", *PASJ International Journal of Computer Science (IIJCS)*, vol. 5, no. 4, 2017.

[38] S. Şen, J. Clark and J. Tapiador, "Security Threats in Mobile Ad Hoc Networks."

[39] P. Kaur and Sukhman, "An Overview on MANET-Advantages, Characteristics and Security Attacks", *International Journal of Computer Applications (0975 – 8887)*, 2016. Available: https://research.ijcaonline.org/icaet2016/number1/icaet018.pdf. [Accessed 28 December 2018].

[40] M. Yadav and N. Uparosiya, "Survey on MANET: Routing Protocols, Advantages, Problems and Security", *International Journal of Innovative Computer Science & Engineering*, vol. 1, no. 2, pp. 12-17, 2014. Available: http://ijicse.in/wp-content/uploads/2014/12/12-17.pdf. [Accessed 28 December 2018].

[41] R. Sheikhl, M. Chandee and D. Mishra, "Security Issues in MANET: A Review", *978-1-4244-7202-4/10/$26.00 ©2010 IEEE*, 2018. [Accessed 28 December 2018].

[42] L. Zhou, Z.J. Haas, Cornell Univ., "Securing ad hoc networks," IEEE Network, Nov/Dec 1999, Volume: 13, Page(s): 24-30, ISSN: 0890-8044

[43] J.-P. HuBaux, L. Buttyan, and S. Capkun., "The quest for security immobile ad hoc network," In Proc. ACM MOBICOM, Oct. 2001.

[44] J. Kong et al., "Providing robust and ubiquitous security support for mobile ad-hoc networks," In Proc. IEEE ICNP, pages 251–260, 2001.

[45] H. Deng, W. Li, Agrawal, D.P., "Routing security in wireless ad hoc networks," Cincinnati Univ., OH, USA; IEEE Communications Magazine, Oct. 2002, Volume: 40, page(s): 70- 75, ISSN: 0163-6804

[46] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding-Royer, "Secure routing protocol for ad hoc networks," In Proc. of 10th IEEE International Conference on Network Protocols, Dept. of Comput. Sci., California Univ., Santa Barbara, CA, USA. 12-15 Nov. 2002, Page(s): 78- 87, ISSN: 1092-1648

[47] H. Yang, H. Luo, F. Ye, S. Lu, L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," In proc. IEE Wireless Communication, UCLA, Los Angeles, CA, USA; volume- 11, Page(s): 38- 47, ISSN: 1536-1284

[48] B. Wu, J. Chen, J. Wu, M. Cardei, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," Department of Computer Science and Engineering, Florida Atlantic University, http://student.fau.edu/jchen8/web/papers/SurveyBookchapter.pdf

[49] H. Kaur and P. Mann, "DETECTION OF BLACK HOLE ATTACK IN MOBILE AD HOC NETWORKS: A SURVEY", *INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS*, vol. 2, no. 3, pp. 58-64, 2014. [Accessed 28 December 2018].

[50] S. Kaushal and R. Aggarwal, "A study of different types of attacks in MANET and performance analysis of AODV protocol against wormhole attack", *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, vol. 4, no. 2, 2015. Available: https://pdfs.semanticscholar.org/8932/8b8d69bea9006c4d5844c7003ee5088d9b59.pdf. [Accessed 28 December 2018].

[51] M. umamaheswari, *Survey on active and passive attacks in Dynamic MobileAd-Hoc Networks*, vol. 3, no. 4, 2012. Available: http://www.academia.edu/2008619/Survey on active and_passive attacks in Dynamic Mobile_Ad-Hoc_Networks. [Accessed 28 December 2018].

[52] A. Kumar, "Security Attacks in Manet - A Review", in *National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing (RTMC) 2011*, 2011.

[53] Gagandeep, Aashima and P. Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 1, no. 5, 2012. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.684.767&rep=rep1&type=pdf. [Accessed 28 December 2018].

[54] R. Bhati and D. Sharma, "A Review on Mobile Ad Hoc Network Attacks with Trust Mechanism", *International*

Journal of Science, Engineering and Technology Research (IJSETR), vol. 5, no. 6, 2016. Available: http://ijsetr.org/wp-content/uploads/2016/06/IJSETR-VOL-5-ISSUE-6-1860-1864.pdf. [Accessed 28 December 2018].

[55] M. Faisal, "ATTACKS IN MANET", *International Journal of Research in Engineering and Technology*, vol. 02, no. 10, pp. 273-276, 2013. Available: 10.15623/ijret.2013.0210040.

[56] P. Chahal, G. Kumar Tak and A. Singh Tomar, "Comparative Analysis of Various Attacks on MANET", *International Journal of Computer Applications*, vol. 111, no. 12, pp. 42-46, 2015. Available: 10.5120/19594-1383.

[57] K. Gupta and P. Mittal, "An Overview of Security in MANET", *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 7, no. 6, pp. 151-156, 2017. Available: 10.23956/ijarcsse/v7i6/0254 [Accessed 28 December 2018].

[58] A. Koul and M. Sharma, "Cumulative Techniques for Overcoming Security Threats in Manets", *International Journal of Computer Network and Information Security*, vol. 7, no. 5, pp. 61-73, 2015. Available: 10.5815/ijcnis.2015.05.08 [Accessed 29 December 2018].

[59] A. Saini and Anu, "Analysis of Security Attacks and Solution on Routing Protocols in MANETs", *International Journal of Computer Science and Mobile Computing*, vol. 5, no. 6, pp. 182-189, 2016. [Accessed 29 December 2018].

[60] J. Ponsam and R. Srinivasan, "A Survey on MANET Security Challenges, Attacks and its Countermeasures", *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, vol. 3, no. 1, 2014. [Accessed 29 December 2018].

[61] H. Bedi, S. Verma and M. Goel, "A Survey on MANET Security Challenges, Attacks and its Countermeasures", *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 5, no. 8, 2016. [Accessed 29 December 2018].

[62] M. Sarkar, and B. D. Roy. "Prevention of sleep deprivation attacks using clustering." Electronics Computer Technology (ICECT), 2011 3rd International Conference on. Vol. 5. IEEE, 2011.

[63] T. Bhattasali, R. Chaki, S. Sanyal, "Sleep Deprivation Attack Detection In Wireless Sensor Network", International Journal of Computer Applications, Vol. 40, No. 15, pp.19-25, February 2012, ISBN: 978-93- 80866-55-8, DOI:10.5120/5056-7374, published by Foundation of Computer Science, New York, USA.

[64] Y.C. Hu, A. Perrig and D. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," Proceedings of the ACM Workshop on Wireless Security (WiSe), SanDiego, California, pp. 30-40, September 2003.

[65] C. E. Perkins and E. M. Royer, "Ad Hoc On-Demand Distance Vector Routing," Proceedings of IEEE Workshop on Mobile Computing Systems and Applications 1999, pp. 90-100, February 1999.