Indonesian Journal of Electrical Engineering and Computer Science
Vol. 12, No. 2, November 2018, pp. 832~842
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v12.i2.pp832-842

A Survey on MANETs: Architecture, Evolution, Applications, Security Issues and Solutions

Burhan Ul Islam Khan, Rashidah Funke Olanrewaju, Farhat Anwar, Athaur Rahman Najeeb, Mashkuri Yaacob
Department of Electrical & Computer Engineering, Kulliyyah of Engineering, IIUM Malaysia

Article Info

Article history:

Received May 24, 2018
Revised Jul 25, 2018
Accepted Aug 8, 2018

Keywords:

Architecture
Issues
Mobile ad hoc network
Node misbehaviour
Security

ABSTRACT

Mobile ad hoc networks or MANETs, also referred to as mobile mesh networks at times, are self-configuring networks of mobile devices that are joined using wireless channels. These represent convoluted distributed systems comprising of wireless mobile nodes which are free to move and self-organise dynamically into temporary and arbitrary, ad hoc topologies. This makes it possible for devices as well as people to internetwork seamlessly in such regions that have no communication infrastructure in place. Conventionally, the single communication networking application following the ad hoc concept had been tactical networks. Lately, new technologies have been introduced such as IEEE 802.11, Hyperlan and Bluetooth that are assisting in the deployment of commercial MANETs external to the military realm. Such topical evolutions infuse a new and rising interest in MANET research and development. This paper provides an overview of the dynamic domain of MANETs. It begins with the discussion on the evolution of MANETs followed by its significance in various fields. Besides, the MANETs have been analysed from the security perspective, particularly the work performed in the node misbehaviour paradigm has been elaborated.

Corresponding Author:

Burhan Ul Islam Khan,
Department of Electrical & Computer Engineering,
Kulliyyah of Engineering, IIUM Malaysia.
Email: burhan.iium@gmail.com

1. INTRODUCTION

The use of wireless cellular systems dates back to the 1970s [1]. Since then, these have been evolving from the first, second, third, fourth to fifth generation wireless systems [2]. A centralised supporting arrangement like that of an access point is required by the wireless networks for their operation. Wireless users are able to remain connected to the wireless systems while roaming using those access points. However, these fixed supporting structures restrict the wireless systems' adaptability, i.e., this technology cannot be employed in regions with no infrastructure in place. The wireless systems of future generations shall need quick and easy deployment of these networks which is not feasible with the standard framework of wireless systems [3]-[6].

As a result of the topical advancements like the introduction of Bluetooth, new wireless systems referred to as MANETs came into existence [7]. A mobile ad-hoc network, also known as short-lived network works devoid of fixed infrastructures. The word ‘ad hoc' is derived from Latin meaning ‘for this or only for this' [8]. MANETs are autonomous systems formed of mobile nodes interconnected via wireless channels with every node functioning as an end system as well as a router for every other node in that network [9]. The mobile nodes in a MANET establish a temporary network dynamically with no centralised administration or fixed infrastructure. With the evolution of wireless networks, the ad hoc potentials are

anticipated to grow in significance. Besides, the technological solutions for supporting more critical, crucial research and development in the future can be envisaged in academy and industry [5].

The rest of the paper is organised into various sections where Section 2 discusses the architecture, history and applications of MANETs. The security challenges posed by MANETs have been illustrated in Section 3 followed by the discussion on security solutions in Section 4. Section 5 explains the game theory and the related work on MANET security has been elucidated in Section 6. Lastly, Section 7 presents the concluding remarks.

2. MOBILE ADHOC NETWORK

Explaining MANET or Mobile Ad hoc Network is a form of wireless network which has attracted utmost attention from numerous researchers. Generally, the mobile nodes in a MANET are autonomously interconnected over wireless links [10]. These nodes are able to directly interact with the nodes that fall in their radio range; however, intermediate nodes are employed for communication with the nodes beyond their radio ranges. This is referred to as multi-hop communication and has been depicted in Figure 1 [11], [12]. Every node works as an autonomous router in a peer-to-peer, distributed mode and produces independent data. There is no requirement of dedicated routers since each node operates as a router forwarding the packets of all the other nodes to enable the exchange of information among mobile nodes [13], [14].

The key benefits provided by MANETs include easy collaboration, adaptability, efficient communication and flexibility in infrastructure-less environments [15]. Despite these pros, MANETs are not devoid of shortcomings since their structure poses various security challenges that are enhanced by multiple intrinsic susceptibilities [16], [17]. The lack of centralised management and monitoring, open access medium, the absence of physical security of MANET members and dynamically changing topologies make MANETs open to intrusions and attacks [18]-[21].

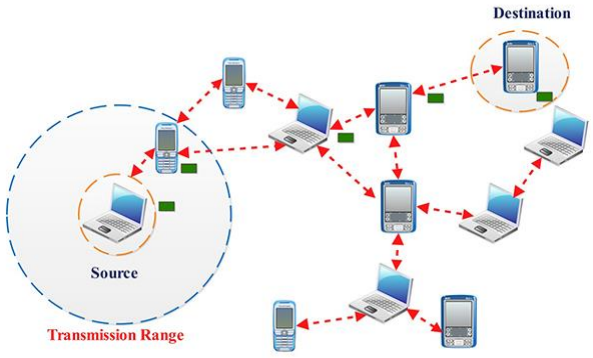

Figure 1. Multi-hop communication in MANETs

2.1. History

The early history of MANETs goes back to 1972, as it was known as Packet Radio Networks or PRNET [22]. The PRNET program was developed under the sponsorship of the United States' Department of Defense. By the use of Arial Location of Hazardous Atmospheres (ALOHA) and Carrier Sense Medium Access (CSMA), a type of distance-vector routing and approaches for medium access control were tested to provide different networking properties in conflicted areas. The PRNET is considered to be the first generation of ad-hoc networks, while SURAN is the second generation that came into existence in the early 80s [23]. The research aimed to develop an infrastructure-less network that can withstand war, and competitive environments. Performance of radio devices was immensely improved as they became cheaper, smaller, and more immune to network attacks [24], [25].

The idea of commercial (non-militarized) MANETs first arose in the 90s as laptops, handphones, and other portable devices came about [26]. During that time, numerous research papers had already discussed the concept of mobile nodes forming a network. Ever since the mid-90s, there were a lot of efforts to regulate ad-hoc networks; hence a MANET working group emerged with a goal to standardise routing protocols for MANETs [25], [27]. Moreover, a medium access protocol that tolerated hidden terminals to create mobile ad-hoc network prototype out of laptops and 802.11 PCMCIA cards, which also was based on avoiding collisions was standardised by a group of IEEE 802.11 subcommittee. Bluetooth was one of the standards that were researched, which helped in the development of MANETs, and so did Hyperlan [28].

The era as mentioned earlier would form what was characterised as the third generation of ad hoc network which also includes present developments and research work on MANETs [29].

2.2. MANET Applications

Conventionally, MANETs were used as a means of communication in environments that were categorised as rough, and tragic where it is difficult to set up a complete communication network, such as combat zones, disaster recovery, rescue missions, deserted areas and more [30]. As MANETs are dynamically formed meaning there is no need for physical connections or centralised base/station since communication depends only on the nodes forming a MANET. The nodes act as transceivers, in other words, they can transmit and receive data simultaneously as mentioned in [4]. Various applications of mobile ad-hoc networks Figure 2 have been enumerated below [31]-[34]:

a) Tactical Networks: Automated battlefields, military communication, etc.
b) Location Aware Services: Advertising location-specific services, automatic call forwarding, Location-based travel guide, etc.
c) Sensor Networks: Remote sensors for weather, earth activities, etc.
d) Educational Applications: Setting up virtual conferences and classrooms.
e) Emergency Services: Commando operations, crowd control, disaster recovery (in times of floods, earthquakes, etc.), etc.
f) Entertainment: Robotic pets, multi-user games, etc.

Figure 2. MANET's applications

3. SECURITY ISSUES IN MANETS

One of the most predominant fields of study in the recent years involves Mobile Ad Hoc Network, also known as MANET. The interest in Mobile Ad Hoc Networks is due to the predicaments it presents to related protocols [25]. In addition to the enhancements, it adds to wireless infrastructure-less networks [11]. In contrast to centre based wireless networks where all nodes have to be connected to a middle point in order to communicate with each other successfully, MANET does not require an access point or a centralised station for its nodes to communicate. Mobile ad hoc network or MANET is an infrastructure-less network, where each node functions as a router allowing the network to possess a dynamic topology where individual nodes have the freedom to move freely. The upsurge of portable, affordable, and technologically advanced devices in markets make Ad Hoc Networks one of the fastest growing networks [25].

The lack of physical organisation makes MANET prone to malicious attacks, and security breaches [35]-[37]. The nature of these attacks can either be internal or external [38]. Examples of external attacks are the denial of service, congested links, as well as false routing information attacks, while internal attacks are exemplified in malicious nodes mimicking regular nodes to access confidential information [11]. This can be done after the malicious node ultimately settles in a network as initially, it will participate in all network activities as a genuine node. These are few attacks that can be found in a MANET.

a) Denial of Service attack

The attackers aim in this particular case to jam the node or the network as a whole, which leads to the unavailability of the attacked node or network. Radio signals are exploited to block the victim node causing unavailability in addition to battery drainage [39].

b) Eavesdropping

Eavesdropping is considered an inactive attack, as the malicious node will examine all the data packets passed through it to gain insight into the network [40]. Usually, attackers are interested in different types of information such as locations, passcodes, and so on.

c) Impersonation

Impersonation takes place when an attacker node acts as a genuine node in a network to gain confidence and trust [41]. In such case where the verification mechanism is not sound, the attacker can bypass it which enables access to confidential data, as well as a chance to monitor traffic in the network [42].

The consequences of these security breaches can lead to continuous intermissions of communications decreasing the efficiency of any network. Such a setback can be caused by the infrastructure-less nature of MANET, which raises the security issue of MANET in regard to authentication and authorisation of nodes. As mentioned above, communication in MANET occurs in a dynamic fashion, which infers that the route taken by sent data from a source to a destination depends on the intermediate nodes that connect both ends. Hence, a characterisation of the used intermediate nodes is required to lessen the security breaches and malicious attacks on a MANET [43]. In general, nodes can be characterised into four categories regular node, selfish node, erroneous node, and malicious node. A regular node is a node that is open to form a connection with any other nodes to forward or receive data packets. On the other hand, a selfish node is a node that saves resources by not transmitting any data. Erroneous node, however, is a node that has hardware deficiencies that may cause difficulties for regular communication and security protocols. Lastly, the malicious node is characterised by destructive tendencies to steal valuable data or disrupt traffic [11].

The research community has always been keen on researching MANETs due to their outstanding dynamic capabilities. The use of routers is wholly eliminated since nodes can communicate with each other independently. However, the downside of the aforementioned dynamic capabilities is the different security issues that arise in MANETs. Even though there was a lot of research work done in the area of QoS (Quality of service), which include studying packet delivery ratio, latency, bandwidth, etc. On the other hand, security issues, in general, have not encountered any significant strides when it comes to delivering outstanding results [44]. The connection in MANET experiences continuous intermissions that disturb communication tremendously due to the dynamic topology MANETs possess. Besides, MANET security system has a lot of dimensional challenges when it comes to authentication and authorisation that is because of the infrastructure-less nature of MANETs. The issue of analysing the behaviour of the node where nodes can be pictured as phones, laptops, personal computers, or computing devices, in general, is proven to be one of the most challenging tasks in solving security issues of networks [4].

To detect misbehaving nodes, recent studies have found the need for some hardware support or peer behaviour evaluation. For instance, reputation-based approaches use a form of eavesdropping that makes use of transmission overhearing, but this can be costly, in addition to the fact that it acquires a significant communication overhead [45]. The following section will shed light on few popular security approaches that have been explored by the research community in the past to mitigate the several security issues MANETs possess [46].

4. VARIOUS SECURITY SOLUTIONS

4.1. Security Through Cryptography

The idea behind cryptography is to encrypt information into strings of unreadable data, which makes it impossible for intercepting entities to gain access to private data [47]. Decryption is the reverse process where the receiver would need a key to make use of the unreadable data received [48]. There are two ways to encrypt data either symmetrically which requires a single key to encrypt/decrypt, or asymmetrically which also needs a key to encrypt/decrypt data; however, the difference is that two different keys are necessary from the sender and receiver [46]. The distinction has been shown in Figure 3.

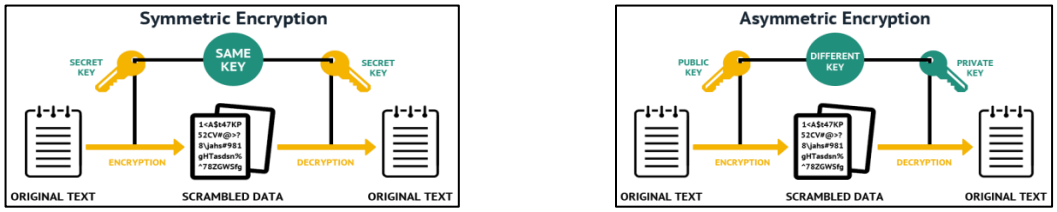

Figure 3. Symmetric vs Asymmetric Cryptography

4.2. Credit-based Methods

There are two credit based models reviewed by [49], these are Packet Purse Model and Packet Trade Model. The Packet Purse Model initially contains all credit necessary within the packet itself, but every time the packet passes by an intermediate node, some of the loaded credit is given to that particular node. It persists until it reaches its destination, or until all the credit finishes. In case all credit was consumed before reaching the target, the packet will be dropped. The second model is Packet Trade; here the intermediate nodes act as traders where they would buy packets from source nodes by giving up some credit, in order to sell it for more credit. The cost of the whole transmission from source to destination is borne by the destination node [50]. According to [45], this kind of a system is usually used to encourage nodes exhibiting selfish behaviour by incentives to provide services or simply forward data packets.

4.3. Reputation-based Methods

Here the reputation is computed depending on the direct interaction with neighbouring nodes, or indirect interaction such as information sent by adjacent nodes about other nodes. The reputation is then used to decide whether it is feasible to forward data through a particular path or not, it can also be used to detect misbehaviour of suspicious nodes. This gathered information is later broadcasted to eliminate such nodes from the network [51]. There are two significant models proposed under this method; the first is Watchdog which is used to detect misbehaviour in MANETs (shown in Figure 4), while the second one is Pathrater which is usually used to mitigate routing misbehaviour in MANETs [45], [52].

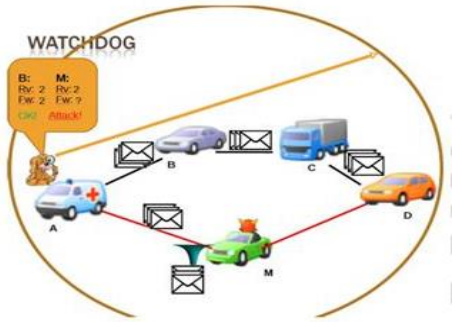

Figure 4. The use of Watchdog mechanism to overhear neighbouring nodes

4.4. Other Security Strategies

There are several security algorithms and models that have been proposed in the past, to warrant the safety of a MANET. These algorithms detect and provide countermeasures towards any malicious threats. Moreover, they lay out the concept behind the security models mentioned earlier, which include certification cryptography systems, swarm intelligence systems, etc. [53].

5. GAME THEORY

While studying some more security mechanisms in MANETs, it was observed that game theory has an unprecedented contribution in the recent past due to the accuracy in its computational efficiency and probabilistic approach.

Game theory can be defined as a mathematical model that analyses interactive decisions in a particular situation that can be called a game. There are two types of game models, cooperative, and non-cooperative [54]. The former is used when the players are bonded to a specified agreement called binding agreement, and the players will act following this agreement. In contrast, the non-cooperative model is applied when there is no binding agreement between the players; this enables the players to change their strategies at any given time. The entities following a non-cooperative model can be called self-enforcing entities. Furthermore, the applications of game theory extend beyond the realm of computers and networks as it has a central place in economic theories. Figure 5 shows some of the applications and fields of studies that incorporate game theory [55].

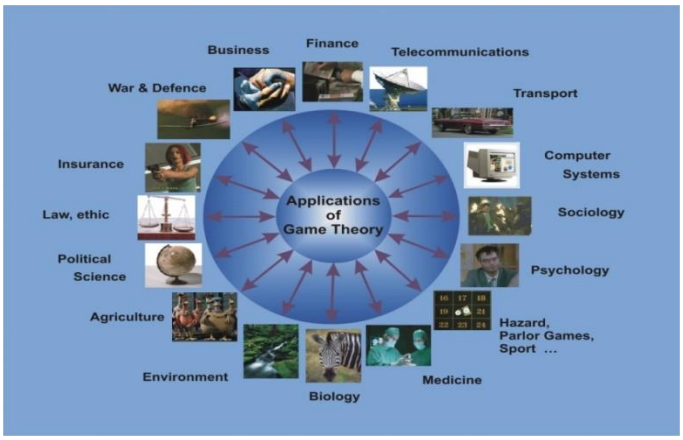

Figure 5. Applications of game theory

6. SECURITY RELATED WORK IN MANETS

Authors in [45] used two techniques to identify what was called a misbehaving node. First, a model called neighbour Overheating based Misbehavior Detection (OMD). This scheme was put forth in order to eavesdrop on surrounding nodes, and compute packet forwarding ratio (PFR) for the node itself, as well as surrounding neighbours. The value of PFR is a vital indicator for the transmitter to identify misbehaving nodes. The second model that was used alongside OMD is Autonomous Agent-based Misbehavior Detection (AAMD). AAMD was used as a criterion to calculate node selection probability since it includes behaviour history of nodes in a network. On the other hand, the model proposed assumes misbehaving nodes as one type meaning that both selfish nodes and malicious nodes are categorised as one. The model also does not consider the possibility of coexistence of malicious nodes and selfish nodes in the same network.

In the study [56], authors deploy misbehaviour detection approach of nodes in a MANET; this is done with the help of two techniques used in tandem. For the first part, the model detects the links associated with any misbehaving nodes, or in other words, it merely identifies the link's misbehaviour by using the 2ACK technique (depicted in Figure 6). The output of this model is later inputted into the second part, which exploits the use of 'Principle of Conservation of flow' also known as (PCF). The 2ACK algorithm is dependent on PCF to identify the specific misbehaving node, as it is limited to determining misbehaving links rather than a particular node. The latter method will be used to identify an individual misbehaving node based on the information of misbehaving connections it receives from 2ACK. However, it would be worth mentioning that their research represents misbehaving nodes as one entity. The model developed in their paper does not take into account the differences between various nodes such as selfish, malicious, and erroneous nodes.

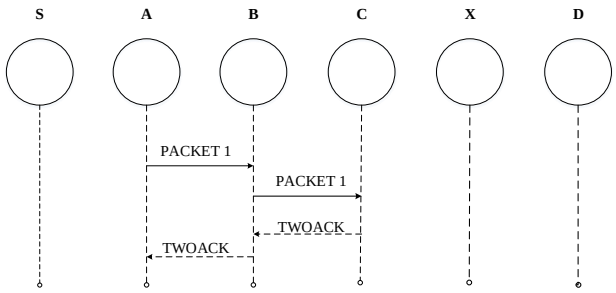

Figure 6. 2ACK scheme

The use of collaborative watchdog approach proved to be useful in the detection of selfish nodes. As authors of [57] elaborated on the watchdog mechanism, which is based on the fast diffusion of selfish nodes awareness. The paper proposed a model that improved the selfish node detection period by using an analytical model, which also attempts to reduce the overhead. A related point to consider is the lack of malicious nodes analysis in this particular paper, as the system was designed specifically to analyse selfish

nodes in a MANET irrespective of other nodes types that may exist. Moreover, the case of false positives in the process of identifying a selfish node from a regular node in a MANET is not considered as a possible case.

Authors in [58] presented a model that used an unconventional approach to tackle the issue of misbehaving nodes in a MANET. As the authors propounded, the noncooperation is usually triggered by the lack of resources; this causes a regular node to turn into a non-cooperative node to save available resources. The proposed model is aimed to minimise resources usage by reducing the massive overhead caused by routing. Yet the focus of this study just like the work mentioned above is dedicated to mitigating the misbehaviour of selfish nodes. There is no mention of malicious nodes that can be motivated by other motives besides saving energy and computational power.

In their study [59], the authors put forth a system that exploits across mechanism of the Watchdog approach, and Collaborative contact-based approach (COCOWA). Few works utilized the use of watchdog alone; however, there are few drawbacks to using the watchdog alone. First, it can fail in the detection of false positive and false negatives. Second, it may inaccurately detect selfish nodes especially in terms of speed, and precision. The proposed model in this paper is based on the dissemination of information about local selfish nodes between regular nodes when they come in contact. Thus, the awareness of selfish nodes in a network can be spread efficiently in terms of time and precision. On the other hand, the authors considered the presence of malicious nodes in the developed model. The only issue was that their role was limited to spreading false negatives, and positives. The COCOWA architecture has been illustrated in Figure 7.

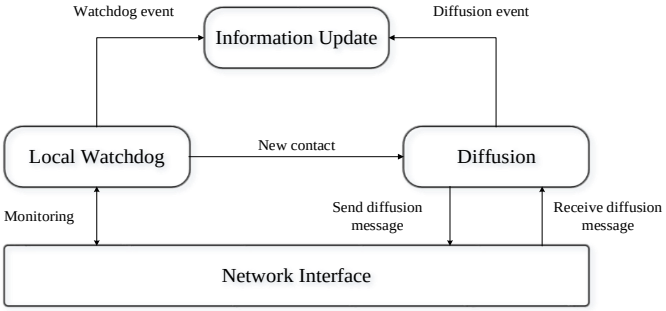

Figure 7. COCOWA Architecture

A modern approach was presented by authors in their research [60], their method utilised the trust based certificate as well as watchdog mechanism. The researchers showed two ways of detecting malicious nodes; these are direct trust and indirect trust. Direct trust makes use of watchdog mechanism to overhear neighbouring nodes for any possible misbehaviour. Indirect trust represents the trust-based method as information about malicious nodes is diffused between trusted nodes. These two methods are used concurrently to insulate malicious nodes in a MANET. The proposed scheme offers a low energy consumption detection of malicious nodes. Nonetheless, the paper focused on the misbehaviour of malicious nodes, but selfish, and erroneous nodes were not studied.

Authors in [61] proposed a mechanism that helps in the prevention of packet dropping by misbehaving nodes; this proposed approach is called Packet Dropping Detection (PDA). For a MANET to be fully connected, it requires the cooperation of nodes in the network to forward data from one point to the other. The collaboration necessitates trusted routes where data packets won't be dropped or tampered with by nodes exhibiting malicious tendencies. Nodes which are willing to cooperate may struggle too if they were being attacked by malicious nodes and this may cause them to partially cooperate or be entirely incapable of cooperating. The paper introduces an algorithm that reports attacker by preventing new nodes from interacting with malicious nodes as well as broadcasting global alarm to notify other nodes in the network.

Furthermore, the detection and removal of misbehaving nodes by using distributed cooperative approach were reviewed in [62]. The model proposed requires all nodes to partake in the process of detecting nodes that exhibit inclinations to misbehave. Nodes in a MANET are expected to share their information of other nodes that includes cooperative nodes and misbehaving nodes as it is needed to facilitate the forwarding of data packets in the network. The reintroduction of a falsely detected node is possible in this work; however, this can be a double-edged sword as it can be taken advantage of by malicious nodes to reenter a MANET. On the other hand, it is evident that the end to end delay would increase considerably on top of the

overhead transmission which would improve as well following this model. The author also elaborates on the use of negative and positive rating structure which may suffer in the face of collusion attacks where malicious nodes would deceive the model's algorithm by broadcasting positive feedback to allow reentry to nodes that share similar intentions.

Game theory was used as an approach to mitigate the security issues in a MANET by helping in the detection of misbehaving nodes. In [63], authors put forth a model that used repeated game forwarding that depended on a global punishment mechanism. This mechanism enforces cooperation between nodes as well as helps to diminish the selfish tendencies exhibited by some of the nodes. The study portrayed misbehaving nodes as intelligent entities that aim to capitalise and take advantage of the system. However, there was no mention of malicious nodes or their effect on the network in other words the coexistence of malicious and selfish nodes wasn't taken into consideration.

Furthermore, game theory approach was utilised based on Route Density Factor, as well as Packet Forward Rate [64]. The study [65] explores a model that identifies selfish nodes and avoids nodes exhibiting malicious behaviour while forwarding packets in a MANET. The model developed aims for minimum idle time and efficient routing in any case where an immediate node exits the transmission range an alternative route is found to facilitate data transmission. The study also considers the existence of the malicious, and selfish nodes in the same system. However, the malicious nodes are deemed to have a fundamental rationale as they can be avoided by the calculation of Route Density Factor.

The findings obtained from the literature review have been summarised in Table 1.

Table 1. Summary of the Findings

Author	Method used	Findings
(Agarwal et al., 2015) [45]	Misbehaviour Detection (OMD) and Autonomous Agent-based Misbehavior Detection (AAMD).	The model proposed assumes misbehaving nodes as one type meaning that both selfish node and malicious node are categorised as one. The model also does not consider the possibility of coexisting malicious nodes, and selfish nodes in the same network.
(Samreen and Narsimha, 2013) [56]	2ACK technique and Principle of Conservation of flow' also known as (PCF)	This article represents misbehaving nodes as one entity. The model developed in this paper does not take into account the differences between selfish, malicious, erroneous nodes etc.
(Hernández-Orallo et al., 2014) [57]	Watchdog mechanism	There is lack of malicious nodes analysis in this particular paper, as the system was designed specifically to analyse selfish nodes in a MANET irrespective of other nodes types that may exist. Moreover, the case of false positives in the process of identifying a selfish node from a regular node in a MANET is not considered as a possible case.
(Akhtar and Sahoo, 2013) [58]	Minimize Resources usage model	There is no mention of malicious nodes which can be motivated by other motives besides saving energy and computational power.
(Hernández-Orallo et al., 2015) [59]	Watchdog approach, and Collaborative contact-based approach	Malicious nodes role was limited to spreading false negatives, and positives. Also, to eliminate the possibility of collusion between the malicious nodes.
(Manoj et al., 2012) [60]	Trust based certificate and watchdog mechanism	Selfish, and erroneous nodes were not studied.
(Prasannavenkatesan et al., 2014) [61]	Packet Dropping Detection (PDA)	The paper introduces an algorithm that reports attacker by preventing new nodes from interacting with malicious nodes as well as broadcasting global alarm to notify other nodes in the network.
(Dadhich et al., 2008) [62]	Distributed cooperative approach	It is evident that the end to end delay would increase considerably on top of the overhead transmission which would improve as well.
(Wang and Wu, 2012) [63]	Global Punishment mechanism	No mention of malicious nodes nor their effect in the network, the coexistence of malicious and selfish nodes wasn't taken into consideration.
(Das et al., 2016) [65]	Game Theory approach	The malicious nodes are considered to have a fundamental rationale.

The work that has been done in the field of profiling misbehaving nodes in a MANET can be described as prolific. A quite number of researchers are interested in this specific field nowadays due to the high potential it possesses. However, the majority of the work done does not consider the existence of malicious nodes, or in case they do their role (malicious nodes) is supposed to be very basic and limited. Besides, the use of game theory for profiling the misbehaving node is thought to be an entirely novel mechanism as there is not a lot of research done in this area.

7. CONCLUSION

Hoc networking forms the foundation for the evolving generations of wireless technology. It is set to become the robust technology for pervasive personal communication owing to its ease of maintenance, self-configuration, inherent flexibility, the absence of built-in infrastructure, substantial cost benefits and self-

administration capacities. The significance and prospects of MANETs are progressively realised by the industry as well as the research community. In the attempt to fulfil these prospects, attending to the open technical and security issues shall play a significant role in applying the MANET potential and acquiring success.

ACKNOWLEDGEMENTS

This work was partially supported by Ministry of Higher Education Malaysia (Kementerian Pendidikan Tinggi) under Fundamental Research Grant Scheme (FRGS) number FRGS13-081-0322 and Research Initiative Grant Scheme (RIGS) number RIGS-16-067-0231.

REFERENCES

[1] Cheng X, Huang X, Du DZ, editors. Ad hoc wireless networking. United States: Springer Science & Business Media; 2013 Dec 1.
[2] Ma Y, Jia Z. Evolution and trends of broadband access technologies and fiber-wireless systems. In: Fiber-Wireless Convergence in Next-Generation Communication Networks. Switzerland: Springer, Cham. 2017: 43-75.
[3] Huang JH, Wang LC, Chang CJ. Architectures and Deployment Strategies for Wireless Mesh Networks. In: Wireless Mesh Networks. Boston, MA: Springer. 2008: 29-56.
[4] Olanrewaju RF, Khan BUI, Anwar F, Khan AR, Shaikh FA, Mir MS. MANET – A Cogitation of its Design and Security Issues. *Middle-East Journal of Scientific Research*. 2016; 24(10): 3094-3107.
[5] Ghosekar P, Katkar G, Ghorpade P. Mobile ad hoc networking: imperatives and challenges. *IJCA Special issue on MANETs*. 2010 Feb; 3: 153-158.
[6] Kumar SA, Babu ES, Nagaraju C, Gopi AP. An empirical critique of on-demand routing protocols against rushing attack in MANET. *International Journal of Electrical and Computer Engineering*. 2015 Oct 1; 5(5) 1102-1110.
[7] Hogie L, Bouvry P, Guinand F. An overview of manets simulation. *Electronic notes in theoretical computer science*. 2006 Mar 9; 150(1): 81-101.
[8] Suri PR, Rani S. Bluetooth network-the adhoc network concept. *Proceedings SoutheastCon, 2007*. IEEE. 2007 Mar 22: 720-720.
[9] Olanrewaju RF, Ali NA, Shah A. ElePSO: energy aware elephant swarm optimization for mobile adhoc network. *Pensee Journal*. 2014; 76(5): 88-103.
[10] Rafsanjani MK, Aliahmadipour L, Javidi MM. A hybrid Intrusion Detection by game theory approaches in MANET. *Indian Journal of Science and Technology*. 2012 Feb 1; 5(2): 2123-2131.
[11] Olanrewaju RF, Anwar F, Shah A. Manifestation and mitigation of node misbehaviour in adhoc networks. *Wulfenia Journal*. 2014 Mar 3; 21(3): 462-470.
[12] Fu Y, Ding Z, Wang D. *A new type of portable MANET terminal with two modes of CSMA and SOTDMA*. 2017 3rd IEEE International Conference on Computer and Communications (ICCC). IEEE. 2017 Dec 13: 443-452.
[13] Misra S, Woungang I, Misra SC, editors. Guide to wireless Ad Hoc networks. London: Springer Science & Business Media. 2009 Mar 2.
[14] Lima MN, Dos Santos AL, Pujolle G. A survey of survivability in mobile ad hoc networks. *IEEE Communications Surveys & Tutorials*. 2009 Jan 3; 11(1): 66-77.
[15] Movahedi Z, Hosseini Z, Bayan F, Pujolle G. Trust-distortion resistant trust management frameworks on mobile ad hoc networks: A survey. *IEEE Communications Surveys & Tutorials*. 2016 Jan 1; 18(2): 1287-1309.
[16] Khan BUI, Olanrewaju RF, Mir RN, Baba A, Adebayo BW. Strategic Profiling for Behaviour Visualization of Malicious Node in Manets Using Game Theory. *Journal of Theoretical & Applied Information Technology*. 2015 Jul 10; 77(1): 25-43.
[17] Reji M, Raja PK, Bhagyalakshmi M. Evaluation of feature reduction using principal component analysis and sequential pattern matching for MANET. *International Journal of Electrical and Computer Engineering (IJECE)*. 2017 Jun 1; 7(3): 1228-1239.
[18] Chang JM, Tsou PC, Woungang I, Chao HC, Lai CF. Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. *IEEE Systems Journal*. 2015 Mar; 9(1): 65-75.
[19] Mitrokotsa A, Komninos N, Douligeris C. *Intrusion detection with neural networks and watermarking techniques for MANET*. IEEE International Conference on Pervasive Services. IEEE. 2007 Jul 15: 118-127.
[20] Olanrewaju RF, Khan BU, Mir RN, Shah A. Behaviour visualization for malicious-attacker node collusion in MANET based on probabilistic approach. *American Journal of Computer Science and Engineering*. 2015 Mar 17; 2(2): 10-19.
[21] Javidi M, Aliahmadipour L. Game Theory Approaches in Taxonomy of Intrusion Detection for MANETs. *Computer Engineering and Applications Journal*. 2015; 4(1): 31-41.
[22] Chigra YB, Ghadi A, Bouhorma M. *Taxonomy of Routing Protocols in MANETs*. International Conference on Advanced Information Technology, Services and Systems. Springer, Cham. 2017 Apr 14: 280-288.
[23] Song L, Wichman R, Li Y, Han Z. Full-Duplex Communications and Networks. United Kingdom: Cambridge University Press; 2017 Feb 28.
[24] Taneja K, Patel RB. *Mobile Ad hoc Networks: Challenges and Future*. Proceedings of National Conference on Challenges & Opportunities in Information Technology (COIT-2007). 2007 Mar 23; 133-135.

[25] Bang AO, Ramteke PL. Manet: history, challenges and applications. *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*. 2013 Sep; 2(9): 249-251.
[26] Xu S, Mu Y, Susilo W. *Efficient authentication scheme for routing in mobile ad hoc networks*. International Conference on Embedded and Ubiquitous Computing. Berlin, Heidelberg: Springer. 2005 Dec 6: 854-863.
[27] Jabbar WA, Ismail M, Nordin R, Arif S. Power-efficient routing schemes for MANETs: a survey and open issues. *Wireless Networks*. 2017 Aug 1; 23(6): 1917-1952.
[28] Chlamtac I, Conti M, Liu JJ. Mobile ad hoc networking: imperatives and challenges. *Ad hoc networks*. 2003 Jul 1; 1(1): 13-64.
[29] Ramanathan R, Redi J. A brief overview of ad hoc networks: challenges and directions. *IEEE communications Magazine*. 2002 May; 40(5): 20-22.
[30] Niemegeers IG, De Groot SH. From personal area networks to personal networks: A user oriented approach. *Wireless Personal Communications*. 2002 Aug 1; 22(2): 175-86.
[31] Gris M, Yang G. Mobile Computing, Applications, and Services. Berlin, Heidelberg: Springer Berlin Heidelberg; 2012.
[32] Khan BU, Olanrewaju RF, Mir RN, Yusoff SH, Sanni ML. Trust and Resource Oriented Communication Scheme in Mobile Ad Hoc Networks. In: Proceedings of SAI Intelligent Systems Conference. Switzerland: Springer, Cham; 2016 Sep 21: 414-430.
[33] Kumar JS, Sandeep J. Does MANET Have Senses?–An Intellectual Approach. *Procedia engineering*. 2012 Jan 1; 38: 1415-1431.
[34] Khan BU, Zulkurnain NF, Olanrewaju RF, Nissar G, Baba AM, Lone SA. JIR2TA: Joint Invocation of Resource-Based Thresholding and Trust-Oriented Authentication in Mobile Adhoc Network. In: Proceedings of SAI Intelligent Systems Conference. Switzerland: Springer, Cham; 2016 Sep 21: 689-701.
[35] Moudni H, Er-rouidi M, Mouncif H, El Hadadi B. *Modified AODV routing protocol to improve security and performance against black hole attack*. 2016 International Conference on Information Technology for Organizations Development (IT4OD). IEEE. 2016 Mar 30: 1-7.
[36] Khan BU, Olanrewaju RF, Baba AM, Zulkarnain NF, Lone SA. *STCM: Secured Trust-Based Communication Method in Vulnerable Mobile Adhoc Network*. 9th International Conference on Robotic, Vision, Signal Processing and Power Applications. Singapore: Springer; 2017: 149-161.
[37] Hussain MA. A novel approach certificate revocation in MANET using fuzzy logic. *Indonesian Journal of Electrical Engineering and Computer Science*. 2018 May 1; 10(2): 654-663.
[38] Olanrewaju RF, Khan BU, Najeeb AR, Zahir KN, Hussain S. Snort-based smart and swift intrusion detection system. *Indian Journal of Science and Technology*. 2018 Jan 14; 11(4): 1-9.
[39] Alharbi A. Security Issues in Wireless Sensor Networks. *Indian Journal of Science and Technology*. 2017; 10(25): 1-5.
[40] Zhang P, Lin C. Security Threats in Network Coding. In: Security in Network Coding. Switzerland: Springer, Cham; 2016: 9-19.
[41] Joshi P. Security issues in routing protocols in MANETs at network layer. *Procedia Computer Science*. 2011 Jan 1; 3: 954-960.
[42] Sheikh R, Chande MS, Mishra DK. *Security issues in MANET: A review*. 2010 Seventh International Conference on Wireless and Optical Communications Networks (WOCN). IEEE. 2010 Sep 6: 1-4.
[43] Khan BU, Olanrewaju RF, Mattoo MUI, Aziz AA, Lone SA. Modeling Malicious Multi-Attacker Node Collusion in MANETs Via Game Theory. *Middle-East Journal of Scientific Research*. 2017; 25(3): 568-579.
[44] Khan B, Olanrewaju RF, Baba AM, Mir RN, Lone SA. DTASR: dual threshold-based authentication for secure routing in mobile adhoc network. *World Engineering & Applied Sciences Journal.* 2016; 7(2): 68-73.
[45] Agarwal D, Rout RR, Ravichandra S. *Detection of node-misbehavior using overhearing and autonomous agents in wireless Ad-Hoc networks*. Applications and Innovations in Mobile Computing (AIMoC), 2015. IEEE. 2015 Feb 12: 152-157.
[46] Olanrewaju RF, Habaebi MH. Malicious behaviour of node and its significant security techniques in MANET-a review. *Australian Journal of Basic and Applied Sciences*. 2013; 7(12): 286-293.
[47] Schneier B. Applied cryptography: protocols, algorithms, and source code in C. United Kingdom: John wiley & sons; 2015.
[48] Gawande PD, Suryavanshi Y. *Cryptography based secured advanced on demand routing protocol in MANET's*. 2015 International Conference on Communications and Signal Processing (ICCSP). IEEE. 2015 Apr 2: 1478-1481).
[49] Buttyán L, Hubaux JP. *Enforcing service availability in mobile ad-hoc WANs*. MobiHOC, First Annual Workshop on Mobile and Ad Hoc Networking and Computing, 2000. IEEE. 2000: 87-96.
[50] Barskar R. *A Basic Technology of Cooperation in Mobile Ad Hoc Networks*. International Symposium on Devices MEMS, Intelligent Systems & Communication (ISDMISC). 2011; 1-4.
[51] Rodriguez-Mayol A, Gozalvez J. Reputation based selfishness prevention techniques for mobile ad-hoc networks. *Telecommunication Systems*. 2014 Oct 1; 57(2): 181-195.
[52] Rizvi SS, Edla V, Poudyal S, Nepal R. *Reducing Malicious Behavior of Mobile Nodes in Ad Hoc Networks*. Novel Algorithms and Techniques in Telecommunications, Automation and Industrial Electronics. Dordrecht: Springer; 2008: 526-531.
[53] Krishnappa PK, Babu BP. Investigating open issues in swarm intelligence for mitigating security threats in MANET. *International Journal of Electrical and Computer Engineering*. 2015 Oct 1; 5(5): 1194-1201.
[54] Ilavendhan A, Saruladha K. Comparative study of game theoretic approaches to mitigate network layer attacks in VANETs. *ICT Express*. 2018 Jan 6; 4(1): 46-50.

[55] Straffin PD. Game theory and strategy. Washington, DC: The Mathematical Association of America; 2004.
[56] Samreen S, Narasimha G. *An efficient approach for the detection of node misbehaviour in a MANET based on link misbehaviour*. 2013 IEEE 3rd International Advance Computing Conference (IACC). IEEE. 2013 Feb 22: 588-592.
[57] Hernández-Orallo E, Olmos MD, Cano JC, Calafate CT, Manzoni P. A fast model for evaluating the detection of selfish nodes using a collaborative approach in MANETs. *Wireless personal communications*. 2014 Feb 1; 74(3): 1099-1116.
[58] Akhtar MA, Sahoo G. A novel methodology for securing ad hoc network by friendly group model. In: Computer Networks & Communications (NetCom). New York, NY: Springer; 2013: 23-35.
[59] Hernandez-Orallo E, Olmos MD, Cano JC, Calafate CT, Manzoni P. CoCoWa: A collaborative contact-based watchdog for detecting selfish nodes. *IEEE transactions on mobile computing*. 2015 Jun 1; 14(6): 1162-1175.
[60] Manoj V, Raghavendiran N, Aaqib M, Vijayan R. Trust based certificate authority for detection of malicious nodes in MANET. In: Global trends in computing and communication systems. Berlin, Heidelberg: Springer; 2012: 392-401.
[61] Prasannavenkatesan T, Raja R, Ganeshkumar P. *PDA-misbehaving node detection & prevention for MANETs*. 2014 International Conference on Communications and Signal Processing (ICCSP). IEEE. 2014 Apr 3: 1163-1167.
[62] Dadhich A, Sarje AK, Garg K. *A distributed cooperative approach to improve detection and removal of misbehaving manet nodes*. 3rd International Conference on Communication Systems Software and Middleware and Workshops, COMSWARE. IEEE. 2008 Jan 6: 728-735.
[63] Wang K, Wu M. Nash equilibrium of node cooperation based on metamodel for MANETs. *Journal of Information Science and Engineering*. 2012 Mar 1; 28(2): 317-333.
[64] Sahnoun A, Habbani A, El Abbadi J. A coalition-formation game model for energy-efficient routing in mobile ad-hoc network. *International Journal of Electrical and Computer Engineering (IJECE)*. 2018 Feb 1; 8(1): 26-33.
[65] Das D, Majumder K, Dasgupta A. *A game-theory based secure routing mechanism in mobile ad hoc network*. 2016 International Conference on Computing, Communication and Automation (ICCCA). IEEE. 2016 Apr 29: 437-442.