Global Journal of Engineering and Technology Advances
eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/

(REVIEW ARTICLE)

Check for updates

A survey on security challenges in the current MANET routing protocols

Fridah Chepkemoi Korir * and Wilson Cheruiyot

Jomo Kenyatta University of Science & Technology, Juja, Kenya.

Global Journal of Engineering and Technology Advances, 2022, 12(01), 078–091

Publication history: Received on 10 June 2022; revised on 16 July 2022; accepted on 18 July 2022

Article DOI: https://doi.org/10.30574/gjeta.2022.12.1.0114

Abstract

Wireless communication employs radio technology to facilitate data transmission without any fixed infrastructures. A mobile ad hoc network is an example of this data transmission technique, which comprises of devices such as smart phones, laptops and printers. Some of the key features of mobile ad hoc networks include self-creation, self-organization and also self-administration. Owing to the frequent mobility of the network nodes and the dynamic topology, mobile ad hoc networks are vulnerable to numerous security threats. For instance, the nodes are open and the links can be disconnected, leading to the degradation of network performance. To mitigate these problems, several protocols and techniques have been proposed in literature. This paper provides some detailed review of these protocols, as well as the discussion of other state of the art protocols that have been developed to cope with challenges of the legacy routing and security protocols. These protocols were established to be either proactive or reactive. In addition, it has been noted that these protocols have some merits as well as challenges that may impede their applicability. Consequently, more efficient and secure routing protocols are required for optimal network performance. Therefore, some recommendations are given towards the end of this paper on some features that ideal routing and security protocol should have.

Keywords: Manets; Routing; Protocols; Security; Performance; IoT

1. Introduction

The proliferation of mobile devices has seen the development of many emerging technologies that deploy ad hoc networks for routing among these devices [1]. In this regard, Mobile Ad-hoc Networks (MANETs) refers to a group of mobile devices that communicate with each other using wireless channels. Due to the high mobility of these devices, the MANET connectivity is dynamic in nature. In this scenario, the communication among devices can be accomplished directly or through some multi hop connections. In essence, MANET does not require any infrastructure and hence can be easily implemented [2] as shown in Figure 1.

According to [3], the nodes that make up the MANETs are not stable and their communication range is small. As such, MANETs frequently utilize multi-hop transmission. The interconnection of smart devices yields an Internet of Things (IoT) which create a smart environment when deployed in specific domains. To realize this, MANETs and Wireless Sensor Networks (WSNs) facilitate the creation of an IoT environment [4], [5]. As explained in [6], the combination of IoT and MANETs is frequently utilized to realize smart cities. Here, the communication may be achieved in peer to peer mode and hence can potentially minimize data delays. The shorter communication distance among MANET nodes calls for multi-hop communication. In addition, MANETs are self-configured networks and the message forwarding is dynamic since the nodes in this network can enter and leave the network at any time. Therefore, the network topology is rapidly changing leading to unpredictability [7].

*Corresponding author: Fridah Korir
Jomo Kenyatta University of Science & Technology, Juja, Kenya.

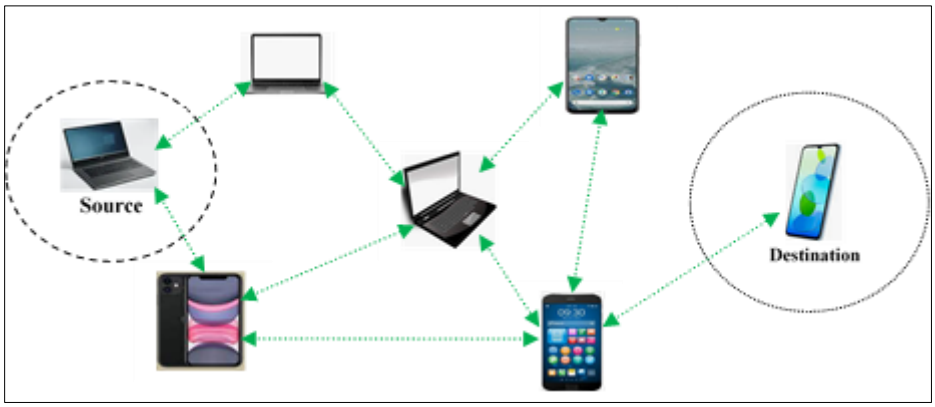

Figure 1 MANET Architecture

Basically, MANETs and WSNs offer communication standards for a myriad of applications via mobility and enhanced usage of resource-constrained [8] devices. In essence, MANET acts as the communication backbone for conveying data from WSN to remote data centers in an effective manner. In this environment, the source and destination nodes may be located in disparate locations and hence data is relayed through intermediate network nodes [9]. Consequently WSN and MANETs have found applications in domains such as military, disaster management, fire disaster management, healthcare, traffic management, waste management, and in smart cities [10]. These domains take advantage of fast, robust and flexible networking mode of MANETs [11]. As explained in [12], MANETs play a critical role in IoT which involves node mobility management. As such, IoT can be thought of as comprising of various wireless networks and MANETs. In this scenario, MANETs offers enhanced connectivity via multi-hop connectivity. In addition, it supports high scaling. To offload high computation complexities [13] from the mobile devices, cloud computing is normally incorporated in these networks. This yields ad hoc based mobile edge computing which provides merits of mobility and high computation power [14], [15].

It is evident that MANETS and WSN in IoT offer many services in numerous application domains. However, lack of centralized control and infrastructure introduces some risks in this communication environment. As such, the interaction among the communicating devices still presents some challenges for desired service provisioning in smart environments. Most of the challenges in MANETs can be contributed to the changing network topology, lack of internal management, large networks and nodes heterogeneity. According to [16], security, privacy and performance are major problems faced by MANETs. Specifically, privacy and confidentiality [17] are basic security requirements that protect location and the data transfer between two communicating parties. According to [1], MANETs are characterized by limited node energy, unstable topologies, low processing capabilities, minimal storage and communication capabilities. All these features affect the general network performance. In addition, the shared communication channels may result in noise, interferences and fading of the transmitted signals. Moreover, MANET nodes are open without any boundary that makes them vulnerable to network security threats or attacks.

Energy constraints are another major challenge in MANETs due to lack of permanent supply of power to the devices. In addition, frequent node mobility that can divert communication links to other nodes, resulting in low throughput. Owing to low storage capacities at the nodes, the battery power can be easily depleted especially in multi-hop communications environment. According to [18], node mobility and their wider dispersion within the network can be a source of insecurities. Frequent packet drop that lead to lower throughput is another major performance issue that is yet to be solved in these networks. As explained in [19], gray-hole attacks are serious challenges in MANETs. In these attacks, some packets are dropped along the communication path. Misbehavior attacks in MANETs have also been noted to be challenging issues [20]. These misbehaviors can be grouped as selfish, malicious, intentional and unintentional. Basically, both selfish and malicious conducts are regarded as intentional misbehaviors. Whenever a particular network node fails to cooperate, it is regarded as selfish misbehavior, which increases the cost of the network in terms of power utilization and computation process. On the other hand, network breaches and the dropping of packets are treated as malicious misbehaviors. In essence, intentional misbehavior takes place when a node willingly permits it to happen. For instance, node movement and network disconnect may both lead to wrong transmissions.

The routing process in MANETs can also render the network insecure. For instance, packet routing, network management and transmissions is the responsibility of network nodes. Since not all these nodes trustworthy, malicious activities can be perpetrated within the network [21]. As explained in [22] and [23], integrity and confidentiality of the transmission process is paramount. These two security features can easily be compromised by non-direct

communication, unstable topology, network threats, bandwidth differences and network complexities. MANET topology instability has been noted in [24] to facilitate network performance degradation. As discussed in [25], security and performance issues center around computation costs, communication overheads, attacks prevention, and energy consumption. The determination of best routes has been noted to be the source of rapid power depletion in MANETs. In reactive protocols, processing time is normally higher during route determination and packet transmission. Evidently, these two processes consume much time and hence end to end delay may be elongated.

The increased deployments and usage of MANETs has endeared these networks to attackers [26], [27]. For instance, authors in [28] identify wormhole attacks as serious challenge facing these networks. The deployment of large numbers of IoT devices in smart cities has also been noted to increase the surface from which attacks can be launched [29]. As discussed in [30] and [31], these attacks have the potential of slowing down the whole network. In addition, MANET network are more vulnerable to attacks compared to the infrastructure-based networks. Quality of Service (QoS) issues is another challenge in these networks [32] due to low throughputs and high computation complexities. To avert malicious data injections, IoT networks, accusation and voting based schemes are utilized to collect data from sensor nodes. Unfortunately, this data collection technique is vulnerable to cooperative blackmailing attacks. In these attacks, a set of malicious nodes accuse a legitimate node of being malicious. Consequently, the network now considers this legitimate node as being malicious. As pointed out in [33] and [34], continuous co-operative blackmailing attack can potentially bring down the entire network. The vast number of smart city devices has been identified in [35] as being the source of energy, security, bandwidth, latency and availability setbacks. On the other hand, wireless transmission and spontaneous nature of MANETs has been noted in [36] and [37] as being the source of many attacks and security threats such as interception, hijacking, jamming of the network data as well as wormhole attack. In addition, new applications that require high computation power and large memory capacity [38] have been noted to be detrimental. According to [39] and [7] the broadcast nature of MANET networks can lead to security exposures. In addition, the physical open channel [40] utilized in MANET and WSN communication is intrinsically insecure. On the other hand, IoT device heterogeneity as been heighted in [41], [42] and [43] as being a major challenge in these networks, more so in smart cities.

As discussed in [9], black hole attacks are very devastating threats that can severely affect network performance. On the other hand, energy utilization, scalability of WSN and dynamic changes have been noted in [44] as being critical towards reliability and robustness of IoT systems. Therefore, it is important that the deployed routing protocols uphold effectiveness in terms of performance, security, and QoS [45]. In addition, MANET routing protocols should ensure that every node is legitimate so as to boost confidentiality, integrity and thwart both denial of service and packet dropping attacks [46]-[50]. In addition, it is important that Man-in-the-Middle attacks are prevented since they have become more common as the demand for smart and internet gadgets surge [51], [52]. Unfortunately, conventional security measures are no longer effective in MANET [11]. The probable reason is their high computation, storage and communication complexities [53] which are not ideal for MANET devices. Therefore, false routing, selective forwarding and byzantine attacks have continued to wreck havoc in these networks. Authors in [54] explain that although MANETs are easy to install, the nodes are battery powered. Therefore, when some of these nodes run down on battery power, the network balance is disturbed. Security is also identified as another major issue in MANETs, especially when dealing with highly sensitive data transaction [55] [56].

It is evident that upholding high levels of security at high energy efficiencies presents great challenges [57]. This is because of the high computation overheads required for most of the conventional security algorithms. Therefore, an ideal security scheme should be lightweight. It should also be capable of offering protection for the entire protocol stack [58], [59].

This paper is organized as follows: Section 2 discusses the related work, while Section 3 presents and discusses the obtained results. On the other hand, Section 4 offers some recommendations for secure message exchange in MANETs. Towards the end of this paper, Section 5 offers conclusion and future research and directions.

2. Related Work

Many conventional protocols exist for efficiency and security enhancement in MANETs. These routing protocols can either reactive or proactive. Examples of proactive routing protocols include Optimized Linked State Routing Protocol (OLSR), Cluster Head Gateway Switch Routing Protocol (CGSR), Wireless Routing Protocol (WRP), and Destination Sequenced Distance Vector Routing Protocol (DSDV). Reactive protocols do not require determination of the paths in advance. Instead, it is done on demand basis, hence can be regarded as On Demand Routing Protocols. Examples of these reactive routing protocols include Ad Hoc On Demand Distance Vector Routing (AODV, Land Mobile Radio (LMR), Temporary Ordered Routing Algorithm (TORA), and Dynamic Source Routing (DSR). Although OLSR produces

maximum throughput, it experiences high overhead and requires vast storage capacity for unnecessary path information [60]. On the other hand, WRP protocol minimizes the number of hops along the path and also boosts reliability. However, more energy is required when reconnecting the path. On its part, CGSR keeps only the information for the cluster heads hence saves on storage. However, more energy is required to keep the cluster heads details.

TORA changes links as it determines the optimal path, controls the channels, erases unnecessary paths and build routes. However, it does not support multicasting in networks. On its part, AODV is scalable and loop free and supports unicast and multicast packet transmission with minimal packet delay. However, it requires more time on updating the route table. In addition, it calls for intensive processing. Consequently, network performance may degrade as the network expands. On the other hand, DSR is fast in recovering a lost or broken path, employs multipath routing and requires minimal energy. However, more time is required when identifying optimal path, in addition to elongated end to end delays. With DSDV protocol, routes from the source to the destination are available. This reduces the amount of time spent in path determination, hence experiences less delays.

The need to protect data transmitted in MANETs has seen the development of numerous security schemes. For instance, a trust based scheme is presented in [61]. However, this scheme is only suited for addressing single node attacks and hence fails to defend against a group of attacking nodes. Although the heuristic algorithm in [62] succeeds in establishing safest paths from the source to the destination, it fails to eliminate malicious nodes from the network. To solve this challenge, the scheme developed in [63] can be deployed. To counter malicious nodes within the network, a two-phase scheme is presented in [64]. Unfortunately, a malicious node can hijack normal node and shield the surrounding normal nodes such that no node is available for routing. On the other hand, authors in [65] employ ant colony optimization (ACO) for optimal route selection. However, the necessary routes may be dropped in this algorithm. Similarly, the scheme in [66] is dedicated for path selection so as to satisfy QoS constraints. Using this approach, network traffic is minimized while security is enhanced. However, retransmission latencies caused a higher delay in the network during transmission. Another predictive trust-based model is presented in [67] for MANETs, while a hybrid algorithm is presented in [2] for safe and energy-efficient navigation in MANETs. Unfortunately, security issues are not considered in [2]. To bridge this gap, the secure protocol in [68] is presented. Authors in [69] have developed a secure data management approach for MANET enabled smart city. However, path security, node's behavior and communication management inside the smart city are not addressed in this technique. This challenge is effectively handled by the scheme in [70]. To uphold the privacy of IoT devices at edge nodes, a genetic algorithm is introduced in [71]. Unfortunately, this technique is shown to provide only surface layer security to the network entities. The topology hiding multipath routing protocol presented in [72] can potentially address the issues in [71] since it is shown to offer perfect confidentiality to the network entities. Similarly, the whale optimization algorithm in [73] can be deployed to enhance trust during the routing process. On the other hand, wormhole attack detection algorithm is presented in [74] while the scheme in [75] is introduced to offer enhanced security.

To enhance QoS in industrial IoT, a trust evaluation mechanism is presented in [76]. However, only the internal attacks present in IoT network are considered in this protocol. Therefore, external attacks instigated by an outside malicious entity cannot be identified and isolated. Although the protocol in [77] can effectively thwart wormhole attacks, this approach delimits the maximum distance that a packet can take in the transmission. On the other hand, authors in [78] have presented a clustering technique to analyze the pattern of the external and internal intruder and effectively find the black hole attack. Unfortunately, this scheme is not scalable for a large number of nodes. To enhance throughput in fog-based MANET, authors in [79] have presented an enhanced Ad hoc on demand distance vector (AODV) routing protocol. However, this protocol focuses only on the attacks on source node. In addition, chances of having a corporation among the attacker nodes are not considered. To curb this challenge, the predictive route model developed in [80] can be utilized. Authors in [81] have introduced a novel wormhole attack detection technique. Unfortunately, this scheme may be vulnerable to de-synchronization [82] attacks. To address this issue, authors in [83] have introduced a trust-based, energy-efficient multipath routing algorithm. On the other hand, authors in [84] have introduced a protocol that is shown to protect against packet loss attacks, using the concept of trustworthiness. Similarly, a single black hole attack prevention technique is presented in [85]. To boost data transmission without any interruption, a trust and novel key-based technique is developed in [86]. However, this scheme incurs long latencies during active attack scenario. Similarly, authors in [87], [88] and [89] have presented a scheme that is shown to boost QoS in MANETs. However, mobile devices are limited in internal resources [90] and hence cannot handle extensive computations in [89]. On the other hand, the authors in [91] have developed a scheme that excludes nodes whose trust value is lower than the threshold. In so doing, potentially malicious nodes are eliminated while the remaining nodes can constitute a trusted network.

To protect against hijacking, jamming and interception attacks, a Markov chain based protocol is presented in [92]. However, the performance of this scheme is adversely affected by heavy network loads. Similarly, a secure autonomic

scheme is developed in [93] for establishing a trusted routing path in MANET. Although the ACO based protocol in [92] incorporates security in its design, it is still hazy. This problem is addressed by the protocol developed in [95]. Similarly, an overhead optimization model is developed in [96]. Unfortunately, the mechanisms deployed complexity reduction may increase the overhead tremendously. To curb wormhole attacks, a directional antennas based protocol is introduced in [97]. Unfortunately, this scheme only prevents the kind of wormhole attacks in which malicious nodes try to deceive two nodes into believing that they are neighbours. To boost security and energy efficiency, a multipath routing protocol is developed in [98]. However, the behavior of this protocol is not investigated in the presence of traffic, mobility, and transmission range. On the other hand, fluctuating topology based protocol is introduced in [99] for securing the key exchange process. Similarly, a trust based system is developed in [100] for black-hole attack prevention. However, this approach increases the computational overhead [101] and may lead to resource unavailability. Although the scheme in [102] results in the reduction of energy, security and privacy issues are never considered. The protocol in [103] potentially addresses this issue by offering defense against cooperative black-hole attacks. However, this technique requires passive table updates and may not withstand sudden link failures. To offer energy efficiency, authors in [104] have introduced a novel routing algorithm, while an adaptive approach is presented in [105] to boost trust levels in the network. Based on digital signatures and asymmetric encryption algorithms, a routing protocol is developed in [106] to secure data transmissions. However, the usage of asymmetric algorithms results in high complexities [107]. The scheme resented in [108] can help mitigate this challenge.

To address energy constraints in MANETs, an optimal path selection algorithm is developed in [109]. Although this approach resulted in minimal energy consumption capability and offered an extended lifetime, it failed to address QoS limitations. This issue is addressed by the scheme developed in [110]. On the other hand, a reliability enhancement technique is presented in [111]. However, this algorithm failed to address Sybil attacks where attackers presented a number of identities during the multipath routing. To curb this, a novel security architecture is developed in [112] which is also demonstrated some resilience against black hole attacks. In addition, energy consumption is also minimized. Similarly, a secret group key based security-aware ad-hoc routing protocol is presented in [113] for trust enhancement among nodes. However, this scheme can be compromised by some malicious group members [114].

Apart from the techniques discussed above, pricing-based methods [115], trust based security strategies [116], [117], cryptographic approaches [92], [118] and game-theoretic methods [111], [98] have been presented. However, the computationally intensive nature [119] of the cryptographic methods renders some of these techniques inefficient for MANETs. On the other hand, the schemes based on trust are application-specific and they require tamperproof hardware [92] that limits their practicality. To offer classification and verification of large-scale MANETs, an asymmetric key based protocol is developed in [120]. Here, the team leader issues certificates to all nodes. Unfortunately, the deployed asymmetric keys render this scheme computationally extensive [121]. On the other hand, private key generation (PKG) based scheme is introduced in [122]. However, this scheme is prone to single point of failure [123]. To boost scalability, reliability and availability, a blockchain based scheme is presented in [124]. However, the deployed blockchains have high storage and computation complexities [125]-[127].

It is evident from the discussions above that many schemes have been developed to offer protection to the data exchanged in MANETs. However, most of these schemes require additional hardware, incur high delay and energy, or fail to provide high throughput and packet delivery ratio.

3. Results

The literature reviewed has shown that there are numerous protocols that can be deployed for packet routing in MANETs. However, each of these protocols has a number of performance and security issues that need to be solved. Table 1 below gives a summary of these protocols, including their strengths and weaknesses.

Based on Table 1 and Table 2, it is evident that upholding high levels of security in MANETs presents numerous challenges. It is also clear that the assurance of optimal quality of service during the routing process is still challenging. Therefore, the recommendations in Section 4 below can be formulated.

Table 1 Conventional Routing Protocols

Protocol	Type	Strengths	Weaknesses
TORA	Reactive	Better for determining optimal routes	No support on multicast networks
AODV	Reactive	Scalable, loop free	Delays
DSR	Reactive	Fast in route reconnection.	Delays
DSDV	Proactive	Track the best route	High energy consumption
OLSR	Proactive	Less delay, user friendly	Maximum energy required.
CGSR	Proactive	Saves on storage	Maximum energy required.
NEPSSS		Routing issues managed.	More energy consumed
Formal Modelling		Handles issues related to challenging information.	Dropping of the packets, more energy use.
AOMDV		Minimal energy consumed	Affected by bad reports, packet dropping
Trust Based Approach		Untrusted nodes are recorded.	Dropping of the packets, low security
Trust Based Technique		Low energy consumption	Higher packet drops and network collision.
NTPA		Issues on packet routing are handled.	Maximum energy consumed, packet dropping
Multidimensional Trust Evaluation Security Solution		Challenges of bad nodes are solved.	More energy, drops packets.
Direct and Indirect Trust Calculation		Better throughput.	Network collision, drops packets and low speed.

To address the issues in the protocols in Table 1 above, researchers in both academia and the industry have developed state of the art protocols. However, the attainment of perfect security in MANET at optimal complexities and efficiency still presents some challenges as summarized in Table 2 below.

Table 2 Summary of Challenges of state of the art MANET security protocols

Scheme	Challenges
Bo et al. [61]	Fails to defend against a group of attacking nodes
Fotohi et al. [62]	Fails to eliminate malicious nodes from the network
Selvi et al. [65]	Necessary routes may be dropped
Borkar et al. [66]	High retransmission latencies
Veeraiahet al.[2]	Security issues are not considered
Zhang et al. [69]	Path security, node's behavior and communication management inside the smart city are not addressed
Xu et al. [71]	Provides only surface layer security to the network entities
Wang et al. [76]	Only the internal attacks present in IoT network are considered
Lai, [77]	Delimits the maximum distance that a packet can take in the transmission

Bala et al. [78]	Not scalable for a large number of nodes
Fang et al. [79]	Focuses only on the attacks on source node
Hu et al. [81]	Vulnerable to de-synchronization attacks
Yannam and Prasad, [86]	Incurs long latencies during active attack scenario
Dbouk et al. [89]	Incurs high computation overheads
Sarkar et al. [92]	Performance is adversely affected by heavy network loads
Tianze et al. [96]	Incurs increase the overheads
Manoranjini et al. [100]	Incurs high computational overhead
Abdali et al. [102]	Security and privacy issues are never considered
Dorri, [103]	May not withstand sudden link failures
Rahman and Mahi, [106]	Incurs high computation and communication complexities
Taha et al. [109]	Fails to address QoS limitations
Lou et al. [111]	Cannot withstand Sybil attacks
Kianpishehet al. [113]	Can be compromised by some malicious group members
[Bhattacharya and Sinha, [118]	Computationally intensive
Singh et al. [116], Subba et al. [117]	Require tamperproof hardware, are application-specific
Van et al. [120]	Computationally extensive
Pushpa et al. [122]	Prone to single point of failure
Lwin et al. [124]	Incurs high storage and computation complexities

Recommendations

It is paramount that security be strengthened in MANETs so that the exchanged data is sufficiently protected. This is quite important since MANETs are frequently deployed in sensitive application domains such as in the military. In addition, the deployed security mechanisms should be designed in such a way that performance is not severely affected. In this regard, the following recommendations can be formulated.

- The communication overheads during the authentication process should be kept at minimum. This is because one of the most serious ways in which power is consumed is through message exchanges among the MANET devices. As such, only few messages should be exchanged during the authentication process so as to prevent draining battery power.
- Data protection, access control and identity management should be enforced in MANETs. Doing this will protect the communication process from both internal and external attackers who may be interested in eavesdropping, intercepting, modifying or replaying the transmitted data.
- The design of any routing protocol in MANET should be capable of thwarting typical attacks such as session hijacking, jamming and message interception.
- Owing to the dynamic topology in MANETs, the routing protocols should be designed in such a way that it is highly scalable. This will enable it handle the frequent joining and leaving of the network nodes.
- Due to the integration of MANET and WSN in an IoT environment, a unified framework should be put in place for efficient and secure communication among the intelligent agents.
- To detect any network violations and malicious access, an effective intrusion detection system should be installed in MANETs. This is critical for continuous monitoring of malicious activities within the network.
- Since MANETs have no centralized control, there should be a mechanism through which malicious nodes can be identified from legitimate ones.

- During the deployment of security solutions, special emphasis should be placed on network availability, energy, bandwidth, latency and security. These factors are significant for the preservation of MANET devices battery power. Figure 2 gives a depiction of the proposed data exchange process.

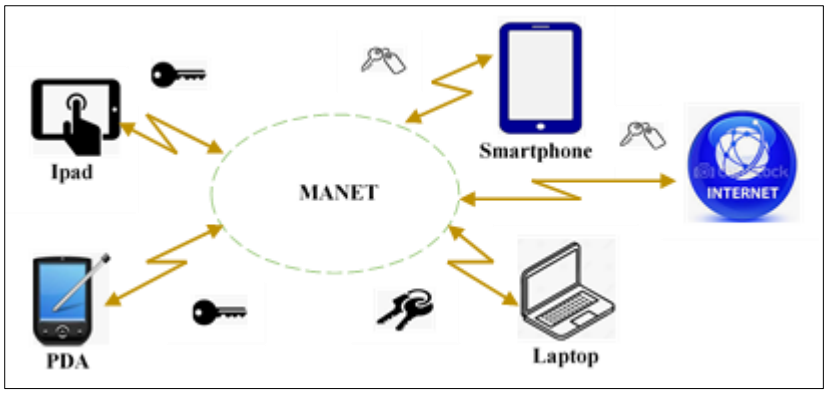

Figure 2 Proposed Secure MANET Communication

As shown in Figure 2, all the communication from the MANET devices are protected by encryption keys. The algorithms for these keys are believed to be strong enough to deter any brute force, dictionary as well as offline password guessing attacks by any polynomial time adversary. Since the MANET may need to establish connections to the public internet, this connection should also be sufficiently protected. This may encompass traffic encryption, filtering as well as access control.

4. Conclusion and future work

For effective packet transmission in MANETs, proper routing techniques should be employed. This paper has discussed the challenges experienced in legacy MANET protocols from the performance and security perspectives. It has been noted that these legacy schemes are classified as being proactive, reactive or hybrid. Proactive techniques have been noted to keep route information in routing table, which ensures that the path is available whenever it is required. In so doing, provides better quality of service. Unfortunately, proactive protocols are not applicable in extended networks. They also consume a lot of energy during the routing process. On the other hand, reactive protocols are used only on demand basis, and therefore save on energy use as well as storage capacity. On the flipside, the determination of optimal paths on demand may delay the routing of the exchanged packets. To curb these challenges, many state of the art protocols have been put forward. Therefore, a review of the state of the art protocols that have been developed to address the issues in legacy protocols has been presented. Unfortunately, these protocols still have numerous setbacks that are yet to be solved. Towards the end of this paper, recommendations are given on how these MANET issues can be effectively addressed. Future work will involve the actual realization of the proposed protocol, which will provide the basis for its evaluation.

Compliance with ethical standards

Acknowledgments

We would like to acknowledge colleagues and the university for the support they offered us during the process of developing this article.

Disclosure of conflict of interest

The authors declare that they have no any conflict of interest.

References

[1] Devi M, Gill NS. Mobile ad hoc networks and routing protocols in IoT enabled. Journal of Engineering and Applied Sciences. 2019; 14(3):802-11.

[2] Veeraiah N, Khalaf OI, Prasad CV, Alotaibi Y, Alsufyani A, Alghamdi SA, Alsufyani N. Trust aware secure energy efficient hybrid protocol for manet. IEEE Access. 2021 Aug 30; 9:120996-1005.

[3] Usha MS, Ravishankar KC. Implementation of trust-based novel approach for security enhancements in MANETs. SN Computer Science. 2021 Jul; 2(4):1-7.

[4] Tripathy BK, Jena SK, Reddy V, Das S, Panda SK. A novel communication framework between MANET and WSN in IoT based smart environment. International Journal of Information Technology. 2021 Jun;13(3):921-31.

[5] Nyakomitta PS, Nyangaresi VO, Ogara SO. Efficient Authentication Algorithm for Secure Remote Access in Wireless Sensor Networks. Journal of Computer Science Research. 2021 Oct; 3(4): 43-50.

[6] Simpson SV, Nagarajan G. A fuzzy based co-operative blackmailing attack detection scheme for edge computing nodes in MANET-IOT environment. Future Generation Computer Systems. 2021 Dec 1;125:544-63.

[7] Amutha S, Balasubramanian K. Secured energy optimized Ad hoc on-demand distance vector routing protocol. Computers & Electrical Engineering. 2018 Nov 1;72:766-73.

[8] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. In The Fifth International Conference on Safety and Security with IoT 2023 (pp. 81-99). Springer, Cham.

[9] Kowsigan M, Rajeshkumar J, Baranidharan B, Prasath N, Nalini S, Venkatachalam K. A novel intrusion detection system to alleviate the black hole attacks to improve the security and performance of the MANET. Wireless Personal Communications. 2021 Apr 26:1-21.

[10] Quy VK, Nam VH, Linh DM, Ban NT, Han ND. A survey of QoS-aware routing protocols for the MANET-WSN convergence scenarios in IoT networks. Wireless Personal Communications. 2021 Sep;120(1):49-62.

[11] Tu J, Tian D, Wang Y. An active-routing authentication scheme in MANET. IEEE Access. 2021 Jan 27; 9:34276-86.

[12] Albeshri A. An image hashing-based authentication and secure group communication scheme for IoT-enabled MANETs. Future Internet. 2021 Jun 27; 13(7):166.

[13] Nyangaresi VO, Ogundoyin SO. Certificate Based Authentication Scheme for Smart Homes. In 2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 202-207). IEEE.

[14] Badii C, Bellini P, Difino A, Nesi P. Smart city IoT platform respecting GDPR privacy and security aspects. IEEE Access. 2020 Jan 22; 8:23601-23.

[15] Wang D, Bai B, Lei K, Zhao W, Yang Y, Han Z. Enhancing information security via physical layer approaches in heterogeneous IoT with multiple access mobile edge computing in smart city. IEEE Access. 2019 May 1; 7:54508-21.

[16] Ramphull D, Mungur A, Armoogum S, Pudaruth S. A review of mobile ad hoc NETwork (MANET) Protocols and their Applications. In 2021 5th international conference on intelligent computing and control systems (ICICCS) 2021 May 6 (pp. 204-211). IEEE.

[17] Nyangaresi VO. A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN COMPUT. SCI. 2022 Jul; 3, 364: 1-16.

[18] Deva Priya M, Janakiraman S, Sandhya G, Aishwaryalakshmi G. Efficient pre-authentication scheme for inter-ASN handover in high mobility MANET. Wireless networks. 2021 Feb;27(2):893-907.

[19] Ourouss K, Naja N, Jamali A. Defending against smart grayhole attack within MANETs: A reputation-based ant colony optimization approach for secure route discovery in DSR protocol. Wireless Personal Communications. 2021 Jan; 116(1):207-26.

[20] Machado C, Westphall CM. Blockchain incentivized data forwarding in MANETs: Strategies and challenges. Ad Hoc Networks. 2021 Jan 1; 110:102321.

[21] Kalime S, Sagar K. A review: secure routing protocols for mobile adhoc networks (MANETs). Journal of Critical Reviews. 2021; 7:8385-93.

[22] Al Sibahee, MA, Nyangaresi VO, Ma J, Abduljabbar ZA. Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things. In 2021 7th EAI International Conference on IoT as a Service (IoTaaS) 2021 Dec 13(pp, 3-18). Springer, Cham.

[23] Srilakshmi U, Alghamdi SA, Vuyyuru VA, Veeraiah N, Alotaibi Y. A secure optimization routing algorithm for mobile ad hoc networks. IEEE Access. 2022 Jan 19; 10:14260-9.

[24] Manvi SS, Tangade S. A survey on authentication schemes in VANETs for secured communication. Vehicular Communications. 2017 Jul 1; 9:19-30.

[25] Nyangaresi VO. ECC based authentication scheme for smart homes. In2021 International Symposium ELMAR 2021 Sep 13 (pp. 5-10). IEEE.

[26] Abd El-Latif AA, Abd-El-Atty B, Mehmood I, Muhammad K, Venegas-Andraca SE, Peng J. Quantum-inspired blockchain-based cybersecurity: securing smart edge utilities in IoT-based smart cities. Information Processing & Management. 2021 Jul 1; 58(4):102549.

[27] Mukherjee S, Biswas GP. Networking for IoT and applications using existing communication technology. Egyptian Informatics Journal. 2018 Jul 1; 19(2):107-27.

[28] Tahboush M, Agoyi M. A hybrid wormhole attack detection in mobile ad-hoc network (MANET). IEEE Access. 2021 Jan 13; 9:11872-83.

[29] Nyangaresi VO. Provably Secure Protocol for 5G HetNets. In2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS) 2021 Nov 1 (pp. 17-22). IEEE.

[30] Ali S, Ahmed A, Raza M. Towards better routing protocols for IoT. In2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET) 2019 Jan 30 (pp. 1-5). IEEE.

[31] Singh P, Khari M, Vimal S. EESSMT: an energy efficient hybrid scheme for securing mobile ad hoc networks using IoT. Wireless Personal Communications. 2021 Aug 22:1-25.

[32] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Jun 25:100210.

[33] Khan LU, Yaqoob I, Tran NH, Kazmi SA, Dang TN, Hong CS. Edge-computing-enabled smart cities: A comprehensive survey. IEEE Internet of Things Journal. 2020 Apr 10;7(10):10200-32.

[34] Xu X, Huang Q, Yin X, Abbasi M, Khosravi MR, Qi L. Intelligent offloading for collaborative smart city services in edge computing. IEEE Internet of Things Journal. 2020 Jun 9; 7(9):7919-27.

[35] Nyangaresi VO. Hardware assisted protocol for attacks prevention in ad hoc networks. InInternational Conference for Emerging Technologies in Computing 2021 Aug 18 (pp. 3-20). Springer, Cham.

[36] Singh R, Singh J, Singh R. WRHT: a hybrid technique for detection of wormhole attack in wireless sensor networks. Mobile Information Systems. 2016 Jan 1; 2016.

[37] Jamali S, Fotohi R, Analoui M. An artificial immune system based method for defense against wormhole attack in mobile adhoc networks. Tabriz Journal of Electrical Engineering. 2018 Feb 20;47(4):1407-19.

[38] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6). IEEE.

[39] Lou W, Liu W, Zhang Y, Fang Y. SPREAD: Improving network security by multipath routing in mobile ad hoc networks. Wireless Networks. 2009 Apr; 15(3):279-94.

[40] Nyangaresi VO, Petrovic N. Efficient PUF based authentication protocol for internet of drones. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[41] Rizzi A, Granato G, Baiocchi A. Frame-by-frame wi-fi attack detection algorithm with scalable and modular machine-learning design. Applied Soft Computing. 2020 Jun 1;91:106188.

[42] Sun Z, Wei M, Zhang Z, Qu G. Secure routing protocol based on multi-objective ant-colony-optimization for wireless sensor networks. Applied Soft Computing. 2019 Apr 1;77:366-75.

[43] Nyangaresi VO, Mohammad Z. Privacy preservation protocol for smart grid networks. In 2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[44] Bessis N, Xhafa F, Varvarigou D, Hill R, Li M, editors. Internet of things and inter-cooperative computational technologies for collective intelligence. Springer Berlin Heidelberg; 2013 Jan 1.

[45] Mohammad Z, Nyangaresi V, Abusukhon A. On the Security of the Standardized MQV Protocol and Its Based Evolution Protocols. In 2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 320-325). IEEE.

[46] Jhaveri RH, Patel SJ, Jinwala DC. DoS attacks in mobile ad hoc networks: A survey. In 2012 second international conference on advanced computing & communication technologies 2012 Jan 7 (pp. 535-541). IEEE.

[47] Verma K, Hasbullah H, Kumar A. Prevention of DoS attacks in VANET. Wireless personal communications. 2013 Nov; 73(1):95-126.

[48] Laxmi V, Lal C, Gaur MS, Mehta D. JellyFish attack: Analysis, detection and countermeasure in TCP-based MANET. Journal of Information Security and Applications. 2015 Jun 1; 22:99-112.

[49] Faghihniya MJ, Hosseini SM, Tahmasebi M. Security upgrade against RREQ flooding attack by using balance index on vehicular ad hoc network. Wireless Networks. 2017 Aug;23(6):1863-74.

[50] Nyangaresi VO, Moundounga AR. Secure Data Exchange Scheme for Smart Grids. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[51] Rout R, Parida P, Alotaibi Y, Alghamdi S, Khalaf OI. Skin lesion extraction using multiscale morphological local variance reconstruction based watershed transform and fast fuzzy C-means clustering. Symmetry. 2021 Nov 3; 13(11):2085.

[52] Jamali S, Fotohi R. Defending against wormhole attack in MANET using an artificial immune system. New Review of Information Networking. 2016 Jul 2;21(2):79-100.

[53] Nyangaresi VO, Morsy MA. Towards Privacy Preservation in Internet of Drones. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[54] Veeraiah N, Krishna BT. An approach for optimal-secure multi-path routing and intrusion detection in MANET. Evolutionary Intelligence. 2020 Mar 26:1-5.

[55] Veeraiah N, Krishna BT. Intrusion detection based on piecewise fuzzy C-means clustering and fuzzy Naïve Bayes rule. Multimedia Research. 2018 Oct;1(1):27-32.

[56] Nyangaresi VO, Alsamhi SH. Towards secure traffic signaling in smart grids. In 2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 196-201). IEEE.

[57] Sarkar S, Datta R. A game theoretic model for stochastic routing in self-organized MANETs. In 2013 IEEE Wireless Communications and Networking Conference (WCNC) 2013 Apr 7 (pp. 1962-1967). IEEE.

[58] Li J, Lewis HW. Fuzzy clustering algorithms—review of the applications. In 2016 IEEE International Conference on Smart Cloud (SmartCloud) 2016 Nov 18 (pp. 282-288). IEEE.

[59] Omollo VN, Chweya RK. Practical Attack on Wi-Fi Protected Access Version 2 Authentication Protocol. Universal Journal of Communications and Network. 2015 Jan; 3(2): 35-40.

[60] Arappali N, Rajendran GB. MANET security routing protocols based on a machine learning technique (Raspberry PIs). Journal of Ambient Intelligence and Humanized Computing. 2021 Jun; 12(6):6317-31.

[61] Wang B, Li M, Jin X, Guo C. A reliable IoT edge computing trust management mechanism for smart cities. IEEE Access. 2020 Mar 6;8:46373-99.

[62] Fotohi R, Nazemi E, Aliee FS. An agent-based self-protective method to secure communication between UAVs in unmanned aerial vehicle networks. Vehicular Communications. 2020 Dec 1; 26:100267.

[63] Nyangaresi VO, Abd-Elnaby M, Eid MM, Nabih Zaki Rashed A. Trusted authority based session key agreement and authentication algorithm for smart grid networks. Transactions on Emerging Telecommunications Technologies. 2022 May 6:e4528.

[64] Faraji-Biregani M, Fotohi R. Secure communication between UAVs using a method based on smart agents in unmanned aerial vehicles. The journal of supercomputing. 2021 May;77(5):5076-103.

[65] Francis Antony Selvi P, Manikandan MS. Ant based multipath backbone routing for load balancing in MANET. IET Communications. 2017 Jan;11(1):136-41.

[66] Borkar GM, Mahajan AR. A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks. Wireless Networks. 2017 Nov;23(8):2455-72.

[67] Alnumay W, Ghosh U, Chatterjee P. A Trust-Based predictive model for mobile ad hoc network in internet of things. Sensors. 2019 Mar 26;19(6):1467.

[68] Alsamhi SH, Shvetsov AV, Kumar S, Shvetsova SV, Alhartomi MA, Hawbani A, Rajput NS, Srivastava S, Saif A, Nyangaresi VO. UAV Computing-Assisted Search and Rescue Mission Framework for Disaster and Harsh Environment Mitigation. Drones. 2022 Jun 22; 6(7):154.

[69] Zhang H, Babar M, Tariq MU, Jan MA, Menon VG, Li X. SafeCity: Toward safe and secured data management design for IoT-enabled smart city planning. IEEE Access. 2020 Aug 6;8:145256-67.

[70] Anantapur M, Patil VC. PUSR: Position Update Secure Routing protocol for MANET. Int. J. Intell. Eng. Syst. 2021 Feb; 14(1):93-102.

[71] Xu X, Liu X, Xu Z, Dai F, Zhang X, Qi L. Trust-oriented IoT service placement for smart cities in edge computing. IEEE Internet of Things Journal. 2019 Dec 12;7(5):4084-91.

[72] Zhang Y, Yan T, Tian J, Hu Q, Wang G, Li Z. TOHIP: A topology-hiding multipath routing protocol in mobile ad hoc networks. Ad hoc networks. 2014 Oct 1; 21:109-22.

[73] Halhalli SR, Sugave SR, Jagdale BN. Optimization driven-based secure routing in MANET using atom whale optimization algorithm. International Journal of Communication Networks and Distributed Systems. 2021;27(1):77-99.

[74] Amish P, Vaghela VB. Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol. Procedia computer science. 2016 Jan 1; 79:700-7.

[75] Nyangaresi VO, Rodrigues AJ, Al Rababah AA. Secure Protocol for Resource-Constrained IoT Device Authentication. International Journal of Interdisciplinary Telecommunications and Networking (IJITN). 2022 Jan 1; 14(1):1-5.

[76] Wang T, Wang P, Cai S, Ma Y, Liu A, Xie M. A unified trustworthy environment establishment based on edge computing in industrial IoT. IEEE Transactions on Industrial Informatics. 2019 Nov 22;16(9):6083-91.

[77] Lai GH. Detection of wormhole attacks on IPv6 mobility-based wireless sensor network. EURASIP Journal on Wireless Communications and Networking. 2016 Dec;2016(1):1-1.

[78] Bala K, Chandra Sekar A, Baskar M, Paramesh J. An efficient multi level intrusion detection system for mobile ad-hoc network using clustering technique. International Journal of Engineering and Advanced Technology (IJEAT). 2019;8(6):1977-85.

[79] Fang W, Zhang W, Xiao J, Yang Y, Chen W. A source anonymity-based lightweight secure AODV protocol for fog-based MANET. Sensors. 2017 Jun 17; 17(6):1421.

[80] Desai AM, Jhaveri RH. Secure routing in mobile Ad hoc networks: A predictive approach. International Journal of Information Technology. 2019 Jun;11(2):345-56.

[81] Hu YC, Perrig A, Johnson DB. Wormhole attacks in wireless networks. IEEE journal on selected areas in communications. 2006 Feb 6; 24(2):370-80.

[82] Nyangaresi VO, Abduljabbar ZA, Refish SH, Al Sibahee MA, Abood EW, Lu S. Anonymous Key Agreement and Mutual Authentication Protocol for Smart Grids. In International Conference on Cognitive Radio Oriented Wireless Networks, International Wireless Internet Conference 2022 (pp. 325-340). Springer, Cham.

[83] Alappatt V, PM JP. Trust-based energy efficient secure multipath routing in MANET using LF-SSO and SH2E. Int. J. Comput. Netw. Appl.. 2021 Aug; 8(4):400.

[84] Eirefaie Y, Nassef L, Saroit IA. Enhancing security of zone-based routing protocol using trust. In2012 8th International Conference on Informatics and Systems (INFOS) 2012 May 14 (pp. NW-32). IEEE.

[85] Nabou A, Laanaoui MD, Ouzzif M. New MPR computation for securing OLSR routing protocol against single black hole attack. Wireless Personal Communications. 2021 Mar;117(2):525-44.

[86] Yannam A, Prasad GV. Trust aware intrusion detection system to defend attacks in MANET. Int J Innov. Technol. Explor. Eng (IJITEE). 2019;8(6):1298-306.

[87] Khan F, Rehman AU, Yahya A, Jan MA, Chuma J, Tan Z, Hussain K. A quality of service-aware secured communication scheme for internet of things-based networks. Sensors. 2019 Oct 6;19(19):4321.

[88] Zhao, H.Y., Wang, J.C., Guan, X., Wang, Z., He, Y.H. and Xie, H.L., 2019, July. Ant colony based energy consumption optimization for mobile iot networks. In 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social

[89] Dbouk T, Mourad A, Otrok H, Tout H, Talhi C. A novel ad-hoc mobile edge cloud offering security services through intelligent resource-aware offloading. IEEE Transactions on Network and Service Management. 2019 Sep 4;16(4):1665-80.

[90] Nyangaresi VO, Abood EW, Abduljabbar ZA, Al Sibahe MA. Energy Efficient WSN Sink-Cloud Server Authentication Protocol. In2021 5th International Conference on Information Systems and Computer Networks (ISCON) 2021 Oct 22 (pp. 1-6). IEEE.

[91] Wang B, Chen XX. Opportunistic routing algorithm based on trust model for ad hoc network. Journal on Communications. 2013;34(9):92-104.

[92] Sarkar S, Datta R. A secure and energy-efficient stochastic multipath routing for self-organized mobile ad hoc networks. Ad Hoc Networks. 2016 Feb 1; 37:209-27.

[93] Dhanya K, Jeyalakshmi C, Balakumar A. A secure autonomic mobile ad-hoc network based trusted routing proposal. In 2019 International Conference on Computer Communication and Informatics (ICCCI) 2019 Jan 23 (pp. 1-6). IEEE.

[94] Nithya R, Amudha K, Musthafa AS, Sharma DK, Ramirez-Asis EH, Velayutham P, Subramaniyaswamy V, Sengan S. An optimized fuzzy based ant colony algorithm for 5G-MANET. CMC-Comput., Mater. Continua. 2022 Jan 1;70(1):1069-87.

[95] Nyakomitta SP, Omollo V. Biometric-Based Authentication Model for E-Card Payment Technology. IOSR Journal of Computer Engineering (IOSRJCE). 2014;16(5):137-44.

[96] Tianze L, Muqing W, Min Z, Wenxing L. An overhead-optimizing task scheduling strategy for ad-hoc based mobile edge computing. IEEE Access. 2017 Mar 3; 5:5609-22.

[97] Hu L, Evans D. Using directional antennas to prevent wormhole attacks. In NDSS 2004 Feb 5 (Vol. 4, pp. 241-245).

[98] Russia S, Anita R. Joint cost and secured node disjoint energy efficient multipath routing in mobile ad hoc network. Wireless Networks. 2017 Oct;23(7):2307-16.

[99] Stulman A, Stulman A. Secured by fluctuating topology using the fluctuating topology of MANETs to secure key exchange. Electronics. 2019 Oct 16; 8(10):1172.

[100] Manoranjini J, Chandrasekar A, Jothi S. Improved QoS and avoidance of black hole attacks in MANET using trust detection framework. Automatika: časopiszaautomatiku, mjerenje, elektroniku, računarstvoikomunikacije. 2019 Jul 28;60(3):274-84.

[101] Nyangaresi VO, Abduljabbar ZA, Abduljabbar ZA. Authentication and Key Agreement Protocol for Secure Traffic Signaling in 5G Networks. In2021 IEEE 2nd International Conference on Signal, Control and Communication (SCC) 2021 Dec 20 (pp. 188-193). IEEE.

[102] Abdali TA, Hassan R, Muniyandi RC, MohdAman AH, Nguyen QN, Al-Khaleefa AS. Optimized particle swarm optimization algorithm for the realization of an enhanced energy-aware location-aided routing protocol in MANET. Information. 2020 Nov 15; 11(11):529.

[103] Dorri A. An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET. Wireless Networks. 2017 Aug;23(6):1767-78.

[104] Dsouza MB, Manjaiah DH. Energy and congestion aware simple ant routing algorithm for MANET. In2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA) 2020 Nov 5 (pp. 744-748). IEEE.

[105] Zhang DG, Gao JX, Liu XH, Zhang T, Zhao DX. Novel approach of distributed & adaptive trust metrics for MANET. Wireless Networks. 2019 Aug;25(6):3587-603.

[106] Rahman MT, Mahi MJ. Proposal for SZRP protocol with the establishment of the salted SHA-256 Bit HMAC PBKDF2 advance security system in a MANET. In2014 International Conference on Electrical Engineering and Information & Communication Technology 2014 Apr 10 (pp. 1-5). IEEE.

[107] Nyangaresi VO, Abduljabbar ZA, Sibahee MA, Abood EW, Abduljaleel IQ. Dynamic Ephemeral and Session Key Generation Protocol for Next Generation Smart Grids. InAd Hoc Networks and Tools for IT 2021 Dec 6 (pp. 188-204). Springer, Cham.

[108] Olanrewaju RF, Anwar F, Mir RN, Yaacob M, Mehraj T. Bayesian signaling game based efficient security model for MANETs. In Future of Information and Communication Conference 2019 Mar 14 (pp. 1106-1122). Springer, Cham.

[109] Taha A, Alsaqour R, Uddin M, Abdelhaq M, Saba T. Energy efficient multipath routing protocol for mobile ad-hoc network using the fitness function. IEEE access. 2017 May 24; 5:10369-81.

[110] Khan BU, Olanrewaju RF, Anwar F, Mir RN. ECM-GT: Design of efficient computational modelling based on game theoretical approach towards enhancing the security solutions in MANET. Int. J. Innov. Technol. Explor. Eng.(IJITEE). 2019 May;8(7):506-19.

[111] Lou W, Liu W, Zhang Y, Fang Y. SPREAD: Improving network security by multipath routing in mobile ad hoc networks. Wireless Networks. 2009 Apr; 15(3):279-94.

[112] Mohammad SN, Singh RP, Dey A, Ahmad SJ. ESMBCRT: enhance security to MANETs against black hole attack using MCR technique. In Innovations in electronics and communication engineering 2019 (pp. 319-326). Springer, Singapore.

[113] Kianpisheh S, Charkari NM, Kargahi M. Ant colony based constrained workflow scheduling for heterogeneous computing systems. Cluster Computing. 2016 Sep; 19(3):1053-70.

[114] Nyangaresi VO, Ibrahim A, Abduljabbar ZA, Hussain MA, Al Sibahee MA, Hussien ZA, Ghrabat MJ. Provably Secure Session Key Agreement Protocol for Unmanned Aerial Vehicles Packet Exchanges. In2021 International Conference on Electrical, Computer and Energy Technologies (ICECET) 2021 Dec 9 (pp. 1-6). IEEE.

[115] Narayandas V, Tiruvayipati S, Hanmandlu M, Thimmareddy L. Anomaly detection system in a cluster based MANET. InComputer Communication, Networking and Internet Security 2017 (pp. 11-21). Springer, Singapore.

[116] Singh O, Singh J, Singh R. Multi-level trust based intelligence intrusion detection system to detect the malicious nodes using elliptic curve cryptography in MANET. Cluster Computing. 2018 Mar;21(1):51-63.

[117] Subba B, Biswas S, Karmakar S. Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation. Engineering Science and Technology, an International Journal. 2016 Jun 1;19(2):782-99.

[118] Bhattacharya A, Sinha K. An efficient protocol for load-balanced multipath routing in mobile ad hoc networks. Ad Hoc Networks. 2017 Aug 1; 63:104-14.

[119] Nyangaresi VO, Abduljabbar ZA, Al Sibahee MA, Abduljaleel IQ, Abood EW. Towards Security and Privacy Preservation in 5G Networks. In2021 29th Telecommunications Forum (TELFOR) 2021 Nov 23 (pp. 1-4). IEEE.

[120] Van Vinh N, Kim MK, Jun H, Tung NQ. Group-based public-key management for self-securing large mobile ad-hoc networks. In2007 International Forum on Strategic Technology 2007 Oct 3 (pp. 250-253). IEEE.

[121] [121] Nyangaresi VO, Rodrigues AJ. Efficient handover protocol for 5G and beyond networks. Computers & Security. 2022 Feb 1; 113:102546.

[122] PushpaLakshmi R, Kumar AV. Cluster based composite key management in mobile ad hoc networks. International Journal of Computer Applications. 2010 Jul; 4(7):30-5.

[123] Nyangaresi VO, Rodrigues AJ, Abeka SO. Machine Learning Protocol for Secure 5G Handovers. International Journal of Wireless Information Networks. 2022 Mar; 29(1):14-35.

[124] Lwin MT, Yim J, Ko YB. Blockchain-based lightweight trust management in mobile ad-hoc networks. Sensors. 2020 Jan 27;20(3):698.

[125] Nyangaresi VO, Rodrigues AJ, Taha NK. Mutual authentication protocol for secure VANET data exchanges. InInternational Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures 2021 May 6 (pp. 58-76). Springer, Cham.

[126] Wang W, Huang H, Zhang L, Su C. Secure and efficient mutual authentication protocol for smart grid under blockchain. Peer-to-Peer Networking and Applications. 2021 Sep;14(5):2681-93.

[127] Wang W, Chen Q, Yin Z, Srivastava G, Gadekallu TR, Alsolami F, Su C. Blockchain and PUF-based lightweight authentication protocol for wireless medical sensor networks. IEEE Internet of Things Journal. 2021 Oct 5; 9(11):8883-91.