ISSN 2278-3091
Volume 9, No.3, May - June 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse175932020.pdf
https://doi.org/10.30534/ijatcse/2020/175932020

A Review on Security-aware Routing Protocols for Mobile Ad hoc Network

Vu Khanh Quy, Pham Minh Chuan, Vi Hoai Nam, Dao Manh Linh
A Hung Yen University of Technology and Education, Vietnam, quyvk@utehy.edu.vn

ABSTRACT
In recent years, Mobile Ad hoc Networks (MANET) have been focused on research and applied in many areas such as military, government and commercial applications. Due to the characteristics of MANET, mobile network nodes can join or leave the network at any time, so a spy network node can be easy to enter into the system and collect vital data. To solve this problem, the design and deployment of reliable routing solutions is a very urgent task in MANET. In this study, we survey the secure-aware routing protocols for MANET proposed in IEEE Xplore Digital Library over the last decade. Based on the results obtained, we suggest future open research directions. We hope that this work will promo for new studies in the field of routing secure-aware for the MANET. The survey results are also an essential basis for the in-depth studies in the military and government applications of the research team.

Key words: Routing Protocol, Security-aware, Mobile Ad hoc Network, MANET.

1. INTRODUCTION

According to the Cisco Visual Index, it is expected that, by 2023, over 70% (5.7 billion) of the global population will have mobile connectivity, up from 66% (5.1 billion) in 2018. Average per capita will have 3.6 devices and connections. Special, the smart devices will be equipped with M2M modules (which is the basic principle forming MANET networks) [1]. Mobile Ad-hoc Networks (MANET), launched in the 1980s, are a set of mobile devices that are capable of self-configuring, establishing, and communicating with each other without relying on base stations [2]. The flexibility and mobility of MANET have made them increasingly popular in a wide range of use domains such as military, government applications. An illustrative example of the rich applications in the MANET networks indicated in Figure 1.

Theoretically, the performance of a MANET network depends on its size, communication model and radio medium. However, in a MANET, dynamic routing features of the system make its performance really low; thus, routing protocols play a particularly vital role in improving the performance of MANET [3]-[5]. Many routing protocols have been proposed for MANET. Among them, AODV (Ad-hoc On-demand Distance Vector) [6] and DSR (Dynamic Source Routing) [7] are the two most well-known protocols. However, these protocols do not yet have security mechanisms and are very vulnerable to cyber-attacks [8]-[10]. To solve these problems, security-aware protocols have been developed to protect routing and application data. In recent years, a lot of routing protocols have been proposed for MANET [28]-[35]. In fact, the deployment of such MANET networks still faces challenges, such as limited physical security, node mobility, and limited resources (processor, power, bandwidth, storage). These issues may affect to the deployment, design as well as performance of a MANET network such as medium access, routing, quality of service (QoS), transport layer protocol, cost function, self-organisation, security, energy efficiency, routing optimal discovery, scalability and deployment consideration [11]-[12]. The protocol design issues are inherently related to

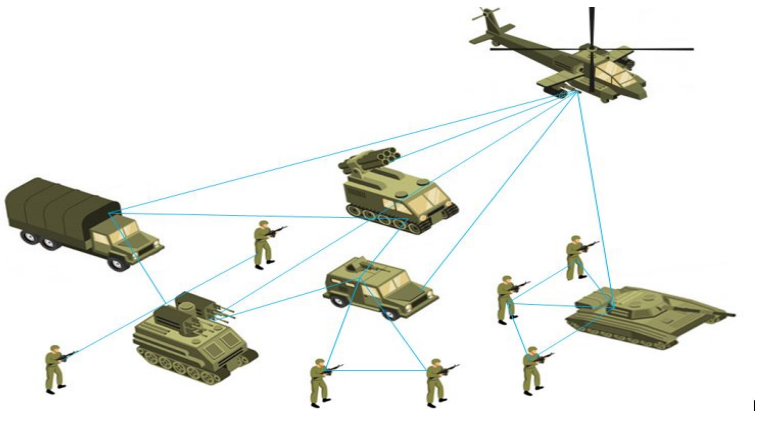

Figure 1: An illustration of the MANET applications in the military area

the underlying MANET applications. Routing protocols are designed for purposes such as quality of service provisioning, energy management and security. In this paper, we focus on the security aspects of the MANET routing protocols.

In this work, we survey existing routing protocols in terms of security and identify their limitations. Besides, we also study different security augmented solutions for these routing protocols. The rest of this paper is organised as follows: In Section 2, we present a classification of existing routing protocols and outline the needed security characteristics to make them secure. A survey salient reactive routing protocols, evaluate their security characteristics and expose existing security limitations are presented in Section 3. In Section 4, we discuss security in hybrid routing protocols and Conclusion.

2. TYPES OF ATTACK REVIEWS

The security of communication in Mobile Ad hoc Networks is vital, especially in military and government applications. The absence of any central coordination mechanism and shared mobile ad hoc network medium makes MANET more vulnerable to digital/cyber attacks than wired networks. These attack methods are generally classified into two types: Passive attacks and Active attacks. Passive attacks do not affect the functionality of networks. Attackers aim to interfere in a network and collect the transmitted data without changing it. If the adversary can interpret the captured data, the requirement of confidentiality is violated. It is difficult to detect Passive attacks because, under attacks, the network operates normally. In general, encryption can be used to combat these type attacks. Active attacks purpose to change or destroy the information of transmission or attempt to influence the normal functioning of the network. Attacks are performed from external systems, called external attacks. If network nodes from within the MANET are involved, the attacks are referred to as internal attack. In order to combat passive and active attacks, a secure MANET is expected to meet the following different security requirements [13]-[14]:

- *Confidentiality*: Only the intended receivers can be able to decryption the transmitted data.
- *Integrity*: Data integrity is ensured when information should be not changed during the transmission process.
- *Availability*: Network services must be available all the time and as well as it should be possible to recover failures to keep the connection stable.
- *Authentication*: Mobile ad hoc nodes must be able to authenticate that the trusted nodes have sent the information. Moreover, each transmitting/receiving node should have its signature.
- *Non-repudiation*: Sender/receiver of a message shall not be able to deny later the message which they sent/received.

In the next section, we present different types of attacks in MANET environment. Most of the research has been focused on addressing issues related to confidentiality and integrity. A lot of solutions have been proposed to address availability and trusted routing, Figure 2, such as follows:

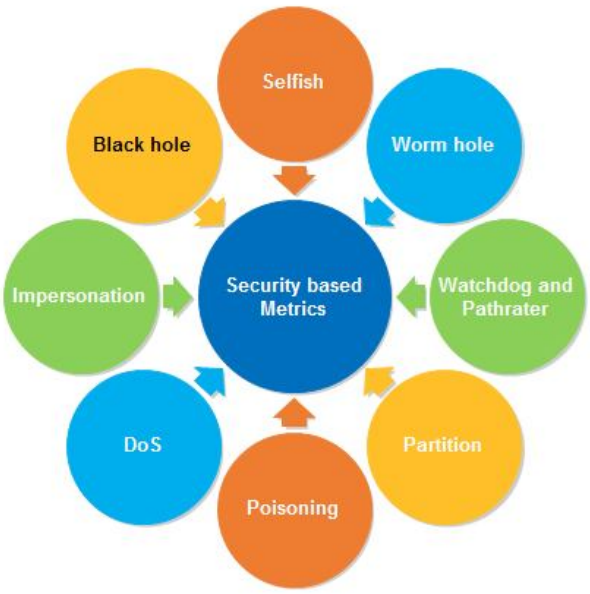

Figure 2: The primary attack methods in Mobile Ad hoc Networks

2.1 External Attack

The external attack is a method which the attacker purpose to making propagate false routing information, make network nodes to denial to provide service normally or congestion. In the mobile ad hoc network environment, external attacks are similar to the regular attacks in the traditional network environments such that the attacker is in the proximity but not an internal network node. Therefore, this method of attack can be prevented and detected by security methods by using a firewall or authentication, which are relatively conventional security solutions.

2.2 Internal Attack

Due to mobile characteristic and the open ad hoc environment in the MANET, the internal attacker (called insider attack) is riskier than the external attack because the compromised or malicious nodes are initially the legitimate users of the MANET network. An attacker can easily pass the authentication and get protection from the security mechanisms. As a result, the attacker can make use of these nodes to gain regular access to the network services that should only be available to the authorised users in the internal MANET. The attacker can use the legal identity provided by the compromised nodes to conceal their malicious behaviours.

1) Black Hole

By send forged routing packets, the attacker could route all packets to some destination, then collect or discard them. By the way, the attacker could cause the route at all nodes to redirect to a node (called a black hole) when in fact the destination is outside the area [15]-[16].

2) Selfish method

In MANET, many of the mobile nodes are lies in the network from that some nodes can be selfish behaviours. Selfishness is

behaviour the node will transfer to other nodes all the work which it can work. Selfish node aims to save its resources to the maximum. This type of misbehaving node discards all incoming packets except those which are destined to it. By dropping control packets, the nodes would not be included in the routing and then be released from being requested to forward data packets [17].

3) Wormhole method

This method using a pair of A and B nodes linked via a private network connection. Every packet that A receives from MANET, A node will forwards through the wormhole to B node, to then be rebroadcast by B node; similarly, B node may send all packets to A node [18].

4) Watchdog and Pathrate method

Watchdog and Pathrater are used in ad hoc routing protocols to keep track of perceived malicious nodes in a blacklist. An attacker may blackmail a trusted node, causing other right nodes to add that node to their blacklists, thus avoiding this node in routes [19]-[20].

5) Partition method

An attacker may try to partition the MANET network by injecting forged routing packets to prevent one set of nodes from reaching another [21].

6) Poisoning method

Routing table poisoning [22]: Routing protocols maintain routing tables which hold information regarding routes of the network. In routing, table poisoning attack the malicious nodes generate and send fabricated signalling traffic, or modify the legal information from other nodes, to create false routes in the routing tables of the participating nodes. An attacker can send not correctly routing updates to actual changes in the topology of the MANET network. Routing table poisoning attack can result in the selection of not optimal routes, creation of routing loops and bottlenecks.

Route Cache Poisoning [23]: This type of attack falls in the category of passive aggression that can occur, especially in DSR protocol due to the mode of updating routing tables. This type of situation arises when routes stored in routing tables is deleted, altered or injected with false data. A network node overhearing any routing packet may add the routes information contained in that the header of the package to its route cache, even if that the node is not on the route from the source node to the destination node. The vulnerability of this system is that an attacker could exploit this route learning method and poison route caches by broadcast a routing packet with a spoofed I.P. address to other nodes in MANET. When modes receive this message, the nodes in MANET would add this new route to their cache and would now communicate other nodes with an error routing table which is support by the malicious node.

7) DoS method

An attacker tries to disturb the communication in a network, for example, by flooding the MANET network with a massive amount of packages. Services offered by the MANET network cannot continue normal working. Its services will be slow down or even stop [24]-[25].

8) Impersonation method

An attacker fakes the identity of an authorised network node, to gain access to network resources; snoops the traffic or disturb the functioning of the MANET network. With a man-in-the-middle attack, an attacker even alters the information transmitted between two network nodes, without letting them know they are not connected directly with each other [26]-[27].

3. REVIEW OF SECURITY-AWARE ROUTING PROTOCOLS

In recent years, due to the practical on-demand to develop smart cities and smart transport systems, some routing protocols have been proposed aimed security-aware for applications, in Table 1, as follows:

To solve the communication security problem in a hostile or suspicious environment, in [28], Karim El Defrawy et al. (2011), proposed an on-demand location-based anonymous routing protocol (PRISM) for MANET which achieves privacy and security against both outsider and insider adversaries. PRISM protocol supports anonymous reactive routing in suspicious location-based MANET. It relies on group signatures to authenticate nodes, ensure the integrity of routing messages while preventing node tracking. PRISM works with any group signature scheme and any location-based forwarding mechanism. Simulation results on the aspects such as security, privacy and performance show that PRISM is more efficient and offers better privacy than existing protocol.

In [29], Karim El Defrawy (2011), authors proposed a privacy-preserving and secure link-state based routing protocol (ALARM) for location-based MANET, which applied in military and law enforcement domains. This protocol uses nodes' current locations to disseminate and construct topology snapshots and forward data securely. It relies on group Signatures to construct one-time pseudonyms used to identify nodes at their present locations. It provides both security and privacy features, including node authentication, data integrity, anonymity, and un-traceability. Besides, ALARM also offers protection against passive and active insider and outsider attacks. The simulation results on aspects such as the overhead and scalability of ALARM show that it performs close to other protocols such as OLSR.

In [30], N. Marchang et al. (2011) proposed a light-weight trust-based AODV routing protocol (Called LTB-AODV) for MANET which operation in hostile environments. Instead of establishing the shortest routes as done in traditional routing protocols, LTB-AODV uses trust-based routing by using the intrusion detection system (IDS) for estimating the trust that one node has for another, consumes limited computational resource. Moreover, unlike other techniques based on monitoring traffic that require a lot of space and time for

Table 1: Security-aware Routing Protocols Indexed in IEEE Xplore Digital Library, 2010-2019

Protocol	Metrics routing	Compare with	Delay	PDR	Energy	Overhead	Special
PRISM [28]	Hop-count	ALARM	NO	NO	NO	NO	YES
ALARM [29]	Link State & Location	OLSR	NO	NO	NO	YES	YES
LTB-AODV [30]	Hop-count	AODV	YES	YES	NO	YES	YES
ALERT [31]	Location	AO2P, ALARM, GPSR	YES	YES	NO	NO	YES
TEAP [32]	Hop-count	MASK	YES	YES	NO	YES	NO
AASR [33]	Hop-count	AODV, ANODR,	YES	NO	NO	NO	YES
SUPERMAN [34]	Link State	IPSec, SAODV, SOLSR	YES	NO	NO	YES	NO
SCOTRES_DSR [35]	Energy, Topology and Channel-Health	A lot of protocols	YES	YES	NO	NO	YES

buffering packets and searching for a packet match, this approach does not require such an overhead. The simulation results on NS2 show the effectiveness of the proposed method.

To offer high anonymity protection at a low cost, in [31], Haiying Shen et al. (2013) propose an Anonymous Location-based Efficient Routing protocol (called ALERT). ALERT dynamically partitions the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non-traceable anonymous route. Besides, it hides the data initiator/receiver among many initiators/receivers to strengthen source and destination anonymity protection. Thus, ALERT offers anonymity protection to sources, destinations, and routes. It also has strategies to counter intersection and timing attacks effectively. Experimental results in terms of anonymity and efficiency show that ALERT achieves better route anonymity protection and lower cost compare with other anonymous routing protocols.

In [32], M. Gunasekaran et al. (2012) proposed a new routing protocol, called TEAP protocol to restrain the misuse of anonymity. This protocol uses two methods: (1) The node A will be notified to other nodes is the attack node if it does not send any cooperative packet after receiving two messages; (2) If the attacker attempts to send multiple claims against a particular node for the same reason it can be termed as the misbehaving node. The TEAP is designed based on broadcast with trapdoor data is a cryptography concept which is used to detect the misbehaving users in the MANET. The simulation results show that the necessity of anonymity in MANET and the effectiveness of the TEAP in achieving anonymity.

Anonymous communications are essential for many applications of MANET, although several anonymous security-aware routing protocols have been proposed, the requirement is not fully satisfied. To solve the problem, in [33], Wei Liu et al. (2014) proposed a new routing protocol, called authenticated anonymous, secure routing protocol (AASR), to satisfy the requirement and defend the attacks. The solution is, the route request packets are verified by a group signature, to protect the potential active attacks without unveiling the node identities. Simulation results show that the effectiveness of the proposed AASR protocol with improved performance as compared to the existing protocols.

In order to protect these MANET networks, security protocols have been developed to safeguard routing and application data. However, these protocols only protect routes or communication, not both. Both secure routing and communication security protocols must be implemented to provide full protection. To solve this problem, in [34], Darren Hurley-Smith et al. (2016) proposed a novel security framework for MANET, called SUPERMAN. The structure is designed to allow existing network and routing protocols to perform their functions while providing node authentication, access control, and communication security mechanisms. The

simulation results show that SUPERMAN outperform compare with IPsec, SAODV and SOLSR protocols for wireless communication security.

With the develope of the Internet of Things (IoT) and cyber-physical systems (CPS), secure routing functionality becomes essential. However, the current solutions focus on a constrain set of network vulnerabilities and do not protect against newer attacks. To solve the problem, In [35], George Hatzivasilis et al. (2017) propose a trust-based routing protocol, called the SCOTRES protocol for ad hoc networks which advances the intelligence of network entities by applying five novel metrics:

(1) The energy metric considers the resource consumption of each node, imposing a similar amount of collaboration and increasing the lifetime of the network.
(2) The topology metric is aware of the nodes' positions and enhances load-balancing.
(3) The channel-health metric provides tolerance in periodic malfunctioning due to bad channel conditions and protects the network against jamming attacks.
(4) The reputation metric evaluates the cooperation of each participant for specific network operation, detecting specialised attacks, while;
(5) The trust metric estimates the overall compliance, safeguarding against combinatorial attacks.

The simulation results on NS2 in terms performance and effectiveness between the proposed protocol compare with six other secure routing schemes in five scenarios indicates that the overhead of the trust system is relatively low and acceptable for the combination of security and node longevity that it is offered.

4. FUTURE DIRECTIONS

In this paper, we have presented different security-aware routing protocols. The secure versions of each of the proposed protocols have also been reviewed. Traditionally, a secure MANET network must be meet security requirements such as Availability, Confidentiality, Integrity, Authentication and non-repudiation. Different digital attacks have been developed to undermine the security of mobile Adhoc networks. These basic attack methods are listed reviewed in Section 2. Table 1 summarises the routing protocols in terms of proposed solutions to withstand different network attacks which indexed in IEEE Xplore digital library in over decade year. Most of the existing protocols have focused on confidentiality and integrity. Few protocols have been done on availability. In more recent research trust-based routing in MANET has gained some interest. Trust is playing a growing security role in an open ad hoc environment where unknown devices can join/leave the system at any time. Also, due to limited processing availability and battery power, existing encryption-based security mechanism appear too burdensome to be considered viable solutions. As presented in research [11], [14]-[18], trust is an assessment based on experience that is shared through the link of the individuals. These shared experiences lead to trust development that augments and decays with time and frequency of interactions. Since communication is becoming pervasive, and pervasive security is an inevitable trend [30],[32], it is only natural to use the notion of pervasive trust where trust relationships are ubiquitous throughout the system. Trust can be used as a measure of certainty for a given operation such as routing in a network. In more recent work, Marchang et al. [30] have proposed a trust-based reactive protocol is the Light-weight trust-based Routing Protocol (LTB-AODV) for Mobile Ad hoc Networks. In [32], M. Gunasekaran et al. has proposed the Trust-Enhanced Anonymous On-demand Routing Protocol (TEAP) for Mobile Ad hoc Networks. The TEAP protocol security is inherently built into the routing protocol where each node evaluates the trust level of its neighbours based on a set of attributes. TEAP trust routing mechanism is based on the basic idea of neighbourhood trust where the trust-level of a node is based on its reputation among its neighbours.

5. CONCLUSION

Due to the ad hoc connection attribute of the nodes, and combined with the mobility characteristics of the nodes in MANET, the security-aware routing for military and government applications for MANET is considered to be a challenging problem. The survey the security-aware routing protocols for military and government application in ad hoc networks shows a common framework to approach solutions for the security-aware path-finding problem in MANET convergence scenarios in IoT network. Over the past decade, from 2010 to the present, researchers have designed and proposed many security-aware routing protocols for ad hoc network (include WSN and MANET). In this study, we conducted a survey of security-aware routing protocols over the last ten years published on the IEEE Xplore Digital Library Database from 2010 to 2019. For each protocol, we performed analysis, compare and discuss open issues. Based on our observations, we have shown a change in research trends over the years as well as determined the promising research directions in the future. This study has primary purpose is to provide an overview of the proposed security-aware routing protocols for the MANET. We hope this work will be promoting the research and development of new security-aware routing protocols in WSN-MANET convergence scenarios in IoT network.

ACKNOWLEDGEMENT

The authors sincerely thank Ass Prof. Dr Nguyen Tien Ban and Ass Prof. Dr Nguyen Dinh Han for their constant support from start to end of this research work.

REFERENCES

1. White paper. Cisco Visual Networking Index: Global Mobile Data Traffic Forecast, 2017–2023. Update 2018. [Online]. Available: https://www.cisco.com
2. Quy V. K., Ban N.T., Nam V.H., Tuan D.M., Han N.D.. Survey of Recent Routing Metrics and Protocols for

Mobile Ad-Hoc Networks,Journal of Communications, 14(2): pp. 110-120, 2019. https://doi.org/10.12720/jcm.14.2.110-120
3. J. P. Josh Kumar, A.Kathirvel.Analysis and Ideas for Improved Routing in MANET, International Journal of Interactive Mobile Technologie, 13(4): pp. 164-177, 2019.
4. V.K. Quy, N.D Han, N.T Ban. A Multi-Metric Routing Protocol to Improve the Achievable Performance of Mobile Ad Hoc Networks, Studies in Computational Intelligence 769, pp. 445-453, 2018.
5. Haider Th. Salim ALRikabi et al., "The Application of Wireless Communication in IoT for Saving Electrical Energy," In International Journal of Interactive Mobile Technologies, 14(1), pp. 152-160, 2020. https://doi.org/10.3991/ijim.v14i01.11538
6. RFC3561. [Online]. Available: https://www.ietf.org
7. RFC4728. [Online]. Available: https://www.ietf.org
8. Quy V.K. and Hung L.N., "A Trade-off between Energy Efficiency and High-Performance in Routing for Mobile Ad hoc Networks," In Journal of Communications, 15(3), pp. 263-269, 2020.
9. W. A. Jabbar, W. K. Saad and M. Ismail, "MEQSA-OLSRv2: A Multicriteria-Based Hybrid Multipath Protocol for Energy-Efficient and QoS-Aware Data Routing in MANET-WSN Convergence Scenarios of IoT," IEEE Access, Vol. 6, pp. 76546-76572, 2018. https://doi.org/10.1109/ACCESS.2018.2882853
10. Quy V.K., Ban N.T., Han N.D., "A High-Performance Routing Protocol for Multimedia Applications in MANET," Journal of Communications, 14(4), pp. 267-274, 2019. DOI: 10.12720/jcm.14.4.267-274.
11. A. Nadeem and M. P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approach for Network Layer Attacks," in IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2027-2045, 2013.
12. G. Ramezan, C. Leung and Z. J. Wang, "A Survey of Secure Routing Protocols in Multi-Hop Cellular Networks," in IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3510-3541, 2018. https://doi.org/10.1109/COMST.2018.2859900
13. A. Nadeem and M. P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks," in IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2027-2045, 2013.
14. M. A. Ferrag, L. Maglaras, A. Ahmim, "Privacy-Preserving Schemes for Ad Hoc Social Networks: A Survey," in IEEE Comm. Surveys & Tutorials, 19(4), pp. 3015-3045, 2017.
15. A. Tsiota, D. Xenakis, N. Passas and L. Merakos, "On Jamming and Black Hole Attacks in Heterogeneous Wireless Networks," in IEEE Transactions on Vehicular Technology, vol. 68, no. 11, pp. 10761-10774, 2019.
16. E. O. Ochola, L. F. Mejaele, M. M. Eloff and J. A. van der Poll, "Manet Reactive Routing Protocols Node Mobility Variation Effect in Analysing the Impact of Black Hole Attack," in SAIEE Africa Research Journal, vol. 108, no. 2, pp. 80-92, 2017. https://doi.org/10.23919/SAIEE.2017.8531629
17. M. Li, S. Salinas, P. Li, J. Sun and X. Huang, "MAC-Layer Selfish Misbehavior in IEEE 802.11 Ad Hoc Networks: Detection and Defense," in IEEE Transactions on Mobile Computing, vol. 14, no. 6, pp. 1203-1217, 2015, DOI: 10.1109/TMC.2014.2348560.
18. F. Nait-Abdesselam, B. Bensaou and T. Taleb, "Detecting and avoiding wormhole attacks in wireless ad hoc networks," in IEEE Communications Magazine, vol. 46, no. 4, pp. 127-133, April 2008.
19. E. Hernandez-Orallo, M. D. Serrat, J. Cano, C. T. Calafate and P. Manzoni, "Improving Selfish Node Detection in MANET Using a Collaborative Watchdog," in IEEE Communications Letters, vol. 16, no. 5, pp. 642-645, 2012.
20. E. Hernández-Orallo, M. D. S. Olmos, J. Cano, C. T. Calafate and P. Manzoni, "CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes," in IEEE Transactions on Mobile Computing, vol. 14, no. 6, pp. 1162-1175, 2015.
21. Z. Zhao, H. Hu, G. Ahn and R. Wu, "Risk-Aware Mitigation for MANET Routing Attacks", in IEEE Trans. on Dependable and Secure Computing, vol. 9, no. 2, pp. 250-260, 2012. https://doi.org/10.1109/TDSC.2011.51
22. S. K. Tetarave, S. Tripathy, E. Kalaimannan, C. John and A. Srivastava, "A Routing Table Poisoning Model for Peer-to-Peer (P2P) Botnets," in IEEE Access, vol. 7, pp. 67983-67995, 2019.
23. H. S. Hmood, Z. Li, H. K. Abdulwahid and Y. Zhang, "Adaptive Caching Approach to Prevent DNS Cache Poisoning Attack," in The Computer Journal, vol. 58, no. 4, pp. 973-985, 2015.
24. D. Gautam and V. Tokekar, "An approach to analyse the impact of DDOS attack on mobile cloud computing," 2017 Inter. Conf. on Information, Communication, Instrumentation and Control, pp. 1-6, 2017.
25. M. Marimuthu and I. Krishnamurthi, "Enhanced OLSR for defence against DOS attack in ad hoc networks," in Journal of Communications and Networks, vol. 15, no. 1, pp. 31-37, 2013. https://doi.org/10.1109/JCN.2013.000007
26. M. M. Rana, K. E. U. Ahmed, N. R. Sumel, M. S. Alam and L. Sarkar, "Security in Ad hoc Networks: A Location-Based Impersonation Detection Method", Inter. Conf. on Computer Engineering and Technology, 2009, pp. 380-384.
27. S. S. Chhatwal and M. Sharma, "Detection of impersonation attack in VANETs using BUCK Filter and VANET Content Fragile Watermarking (VCFW)", 2015 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, pp. 1-5, 2015.
28. [28] Karim El Defrawy, Gene Tsudik, "Privacy-Preserving Location-Based On-Demand Routing in MANET," IEEE Journal on Selected Areas in Communication, Vol. 29, Iss. 10, pp. 1926-1934, 2011.
29. K.E Defrawy, Gene Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANET", IEEE Trans. on Mobile Computing, Vol. 10, Iss 9, pp. 1345-1358, 2011.

30. N. Marchang and R. Datta, "Light-weight trust-based Routing Protocol for Mobile Ad hoc Networks," IET Information Security, Vol. 6, Iss. 2, pp. 77–83, 2011. https://doi.org/10.1049/iet-ifs.2010.0160
31. Haiying Shen and Lianyu Zhao, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANET," IEEE Trans. on Mobile Computing, Vol. 12, No. 6, pp. 1079-1093, 2013.
32. M. Gunasekaran and Kandhasamy Premalatha. TEAP: Trust-Enhanced Anonymous On-demand Routing Protocol for Mobile Ad hoc Networks, *IET Information Security*, Vol. 7, Iss. 3, pp. 203–211, 2013.
33. Wei Liu, Ming Yu, "AASR: Authenticated Anonymous Secure Routing for MANET in Adversarial Environments," IEEE Trans. on Vehicular Tech., Vol. 63, Iss. 9, pp. 4585-4593, 2014.
34. Darren Hurley-Smith, Jodie Wetherall, Andrew Adekunle, "SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad hoc Networks," IEEE Trans. on Mobile Computing, Vol. 16, Iss. 10, pp. 2927-2940, 2017. https://doi.org/10.1109/TMC.2017.2649527
35. George Hatzivasilis et al., "SCOTRES: Secure Routing for IoT and CPS," IEEE Internet of Things Journal, Vol. 4, Iss. 6, pp. 2129-2141, 2017. https://doi.org/10.1109/JIOT.2017.2752801