RESEARCH ARTICLE OPEN ACCESS

Neural Network Based Intrusion Detection System in IoT Environment

Authors Name: Surya Kumar.S [1], Shaikh Muhibudeen.A [1], Santhosh.S[1], Vijayakrishnan.G[1] and Mr.V. Rajakani[2]

*S[1] Students: Department of Electronics and Communication Engg, Anjalai Ammal Mahalingam Engineering College, Thiruvarur(Dt).
Email id: suryakumar65123@gmail.com

**Assistant Professor, Department of Electronics and Communication Engg, Anjalai Ammal Mahalingam Engineering College, Thiruvarur(Dt).
Email id: rajakani.v@gmail.com

ABSTRACT

To examine security concerns in the IoT environment Standard high-end security solutions are insufficient for safeguarding an IoT system due to the low processing power and storage capacity of IoT devices. The IoT network in order to categorize activities as “normal” or “malware” for each tier of the design by establishing a baseline with the intrusion detection datasets. So, we create a security solution based on the Although quite popular for the protection for ad-hoc networks & mitigation techniques only function after the attack has commenced in the Internet of Things network and create an algorithm to overcome the security concerns faced in the IOT environment with a more efficient technique and solving the problems. Our solution assumes no explicit node collaboration, with each node using only internal knowledge gained by routine routing information. The technique was evaluated, allowing for a better understanding of the attack surface and its prevention. Propose a hybrid Intelligent, SDN-enabled model for efficient and early detection in the IoT environment. The proposed Denial of Intrusion Predict and Prevention Node System (DIPS) based intrusion detection and running the processes and the algorithm in matlab software to analyze the working of it.

Keywords: IoT, Adhoc Network, Intrusion Detection System

INTRODUCTION

Due to the widespread availability of mobile IoT devices, mobile ad hoc networks (MANETs) have been widely used for various important applications such as military crisis operations and emergency preparedness and response operations. This is primarily due to their infrastructure less property [1]. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology. MANETs are a kind of IoT based wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. The growth of IoT devices and 802.11/Wi-Fi wireless networking has made MANETs a popular research topic since the mid-1990s. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measures such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput, ability to scale, etc [2].

In a MANET, each node not only works as a host but can also act as a router. While receiving data, nodes also need cooperation with each other to forward the data packets, thereby forming a wireless local area network. These great features also come with serious drawbacks from a security point of view. Many research works have focused on the security of MANETs [3-4]. The lack of any infrastructure added with the dynamic topology feature of MANETs make these networks highly vulnerable to routing attacks such as Intrusion Detection due to attacks (known as variants of blackhole and grayhole attacks). In intrusion process a node transmits a malicious broadcast informing that it has the shortest path to the destination, with the goal of intercepting messages. In also the malicious node is not initially recognized as such since it turns malicious only at a later time, preventing a trust-based security solution from detecting its presence in the network.

Many research works have focused on the security of MANETs. Most of them deal with prevention and detection approaches to combat individual misbehaving nodes. In this regard, the effectiveness of these approaches becomes weak when multiple malicious nodes collude together to initiate a collaborative attack, which may result to more devastating damages to the network.

A with the growth in the use of MANETs, as a standalone networking tool and as the basis for other emerging technologies such as IoT and VANETs the demand for security on this underlying technology is increasing as well. Ubiquitous MANET protocols (i.e., AODV, DSDV, OLSR, etc.), [5] however, were developed with the focus on efficient routing and data transfer performance, not security issues. This, in turn, led to the current situation where these protocols are vulnerable to a multitude of attacks, including spoofing attacks, flooding attacks, wormhole attacks, replay attacks, black-hole attacks, colluding misrelay attacks, and many others.

Therefore the proposed solution based on Denial of Intrusion Predict and Prevention Node System (DIPS) is an algorithm devised to specifically address denial of service (DoS) attack variant called node isolation in OLSR based networks. DIPS's main virtues are its ability to mitigate the node isolation attack by relying solely on internal knowledge acquired by each node during routine routing and in utilizing the same technique used for the attack to prevent damage. As both node isolation and intrusion attacks require similar preliminary steps for attack execution, namely coaxing a victim into appointing the attacker as sole multi-point relay (MPR) node, which is responsible for broadcasting a node's existence to the network, we found DIPS to be a good basis for mitigating the gray-hole attacks as well. As it turns out, although being a sole MPR isn't a requirement for gray-hole attacks to commence, the information provided by DIPS can be used to minimize it as well.

.

I. LITERATURE SURVEY

Many research works have investigated the problem of malicious node detection in MANETs. Most of these solutions deal with the detection of a single malicious node or require enormous resource in terms of time and cost for detecting cooperative blackhole attacks. In addition, some of these methods require specific environments or assumptions in order to operate. In general, detection mechanisms that have been proposed so far can be grouped into two broad categories. 1) Proactive detection schemes that need to constantly detect or monitor nearby nodes. 2) Reactive detection schemes are that trigger only when the destination node detects a significant drop in the packet delivery ratio. Among the above schemes are the ones previously proposed, in which considered as benchmark schemes for performance comparison purposes. In 2ACK scheme for the detection of routing misbehaviour in MANETs. In this scheme, two-hop acknowledgement packets are sent in the opposite direction of the routing path to indicate that the data packets have been successfully received.

The growing development of IoT [6] this paper, we design and develop a novel anomaly-based intrusion detection model for IoT networks. First, a convolutional neural network model is used to create a multiclass classification model. The proposed model is then implemented using convolutional neural networks in 1D, 2D, and 3D. The proposed convolutional neural network model is validated using the BoT-IoT, IoT Network Intrusion, MQTT-IoT-IDS2020, and IoT-23 intrusion detection datasets.

Deep learning [6] is one of the most concerned technology in recent years which realizes automatic feature extraction from raw data. In this article, the integrated model of the convolutional neural network (CNN) and recurrent autoencoder is proposed for anomaly detection. Simple combination of CNN and autoencoder cannot improve classification performance, especially, for time series. Therefore, we utilize the two-stage sliding window in data preprocessing to learn better representations. However [7], cloud-IoT systems increase attacks against web servers, since data centralization carries a more attractive reward. In this article, based on distributed deep learning, we propose a web attack detection system that takes advantage of analyzing URLs. The system is designed to detect web attacks and is deployed on edge devices. The cloud handles the above challenges in the paradigm of the Edge of Things. Multiple concurrent deep models are used to enhance the stability of the system and the convenience in updating.

VANET serves as an application of intelligent transportation system (ITS) that improves traffic safety as well as efficiency. This [8] paper presents an approach for privacy preserving authentication in VANET. Our hybrid approach combines the useful features of both the pseudonym based approaches and the group signature-based approaches to preclude their respective drawbacks. The proposed approach utilizes efficient and light-weight pseudonyms that are not only used for message authentication, but also serve as a trapdoor in order to provide conditional anonymity. We present various attack scenarios that show the resilience of the proposed approach against various security and privacy threats. In [9] Identity-based signature schemes have been used to provide privacy-preserving authentication effectively for VANETs. In such scenario, mutual authentication between vehicles is critical to ensure only legitimate vehicles can involve in the inter-vehicle communication, and how to resist denial-of service attack should be carefully addressed due to the regionally central signature verification in vehicle road side communications.

As a result [9], deduplication system improves storage utilization while reducing reliability. Furthermore, the challenge of privacy for sensitive data also arises when they are outsourced by users to cloud. Aiming to address the above security challenges, this paper makes the first attempt to formalize the notion of distributed reliable deduplication system. We propose new distributed deduplication systems with higher reliability in which the data chunks are distributed across multiple cloud servers. The security requirements of data confidentiality and tag consistency are also achieved by introducing a deterministic secret sharing scheme in distributed storage systems, instead of using convergent encryption as in previous deduplication systems.

In [10], propose an efficient cooperative authentication scheme for VANETs. To reduce the authentication overhead on individual vehicles and shorten the authentication delay, this scheme maximally eliminates redundant authentication efforts on the same message by different vehicles. To further resist various attacks, including free-riding attacks that are launched by selfish vehicles, and encourage cooperation, the scheme uses an evidence-token approach to controlling the authentication workload, without the direct involvement of a trusted authority (TA). When a vehicle passes a roadside unit (RSU), the vehicle obtains an evidence token from the TA via the RSU [11].

In MANETs [12], mobile nodes use wireless devices to create spontaneously a larger network, larger than radio range, in which communication with each other is made possible by the means of routing. One routing protocol for such MANET networks is OLSR, on which this article focuses. We examine the security issues, and describe an architecture including multiple securing mechanisms. In [13] is an open wireless, infrastructure less and topology less network environment in which nodes are free to move anywhere in the network. Various types of protocols are used for communication.

A parameter acknowledgment ratio, i.e., control the ratio of the received data packets for which the acknowledgment is required. This scheme belongs to the class of proactive schemes and, hence produces additional routing overhead regardless of the existence of malicious nodes.

In a prevention mechanism called best-effort fault-tolerant routing (BFTR). Their BFTR scheme uses end-to-end acknowledgements to monitor the quality of the routing path (measured in terms of packet delivery ratio and delay) to be chosen by the destination node. If the behavior of the path deviates from a predefined behavior set for determining "good" routes, the source node uses a new route.

Denial of Intrusion Predict and Prevention Node System

Denial of Intrusion Predict and Prevention Node System (DIPS), is an algorithm devised to specifically address denial of service (DoS) attack variant called node isolation in OLSR based networks. DIPS's main virtues are its ability to mitigate the node isolation attack by relying solely on internal knowledge acquired by each node during routine routing and in utilizing the same technique used for the attack to prevent damage. DIPS verifies the validity of a HELLO message by looking for contradictions between what the message claims and its pre-acquired topological knowledge. According to DIPS Fig. 1 show the proposed system model sole MPRs nominations are allowed only when no contradictions are found. With the presence of contradictions, an MPR can be nominated for all 2-hop neighbours for which the suspected node is the only access point. It cannot, however, be nominated as sole MPR for 2-hop neighbours that can be reached through other paths.

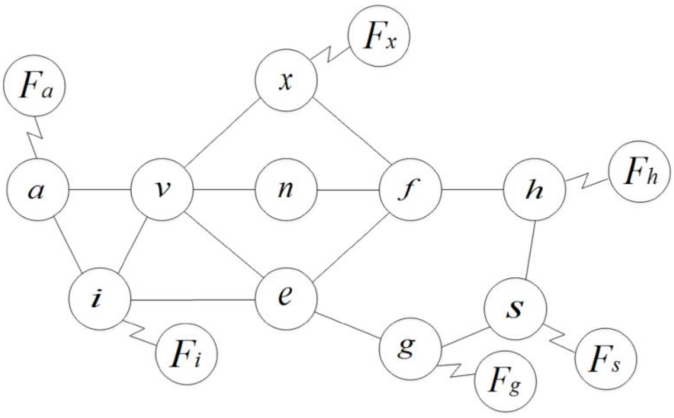

Fig. 1 Illustrating the same network of Figure with the protection of DIPS

DIPS Flow

DIPS proposed in order to address the problem of node isolation in OLSR based networks. It identifies potential malicious nodes trying to falsify HELLO messages using only internal information within the victim, without relying on any centralized or external trusted party. Such early detection prevents a possible attack before it can manifest. DIPS verifies the validity of a HELLO message by looking for contradictions between what the message claims and its pre-acquired topological knowledge. According to DIPS, sole MPRs nominations are allowed only when no contradictions are found. With the presence of contradictions, an MPR can be nominated for all 2-hop neighbors for whom the suspected node is the only access point. It cannot, however, be nominated as sole MPR for 2-hop neighbors that can be reached through other paths.

1) Node Representation (NR)
2) Denial Rules (DR)

Node Representation (NR):

The NR below for the remainder of this work:

- V denote the set of all nodes in the network,
- v, x ∈ V are the victim (as well as/or the receiver) and attacker nodes, respectively,
- Fx is a fictitious node advertised by x,
- ADJ(v) ⊂ V is the set of all 1-hop neighbors of v,
- ADJ2 (v) ⊂ V is the set of all 2-hop neighbors of v,
- MPR (v) ⊆ ADJ (v) is the set of 1-hop nodes of v who appointed v as their MPR, and
- MPR0 (v) ⊆ ADJ (v) is the set of 1-hop nodes who were selected by v as MPRs

Denial Rules:

DIPS define three rules that must be satisfied before a HELLO message sender is considered trustworthy. Only trusted senders can be nominated as sole MPRs for 2-hop nodes that can otherwise be reached, subject to the OLSR protocol. A detailed explanation of these contradiction rules and their inherent logic can be found. When node x advertises a HELLO message containing ADJ(x). For every node z ∈ ADJ(x) ∩ ADJ (v), v should verify that x ∈ ADJ (Z).

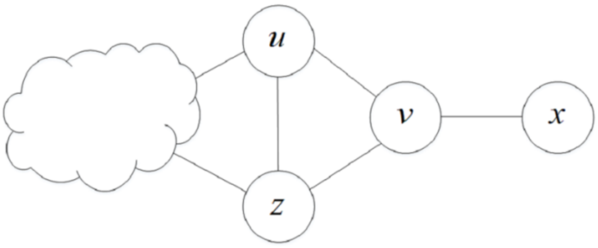

Fig. 2 Intrusion Model

Rule No. 1 can be explained by Fig. 2 in which ADJ (v) = {x, u, z} and x is an attacker. x advertises a HELLO message claiming to know the set of ADJ2 (v) containing z (since z is a v's 2-hop neighbour through u). However, z ∈ ADJ(y) and since z has not included x in its HELLO message, v suspects x.

For each node y mentioned in a HELLO message, v should check whether there exists z ∈ ADJ(y), such that (a) z ∈/ ADJ(x); hence, not mentioned in x's HELLO message and (b) y ∈ ADJ2 (v); thus, z is located at least 3-hops away from v. Once these conditions are fulfilled, (c) it must check if x appointed w ∈ ADJ(x) as MPR for covering z.

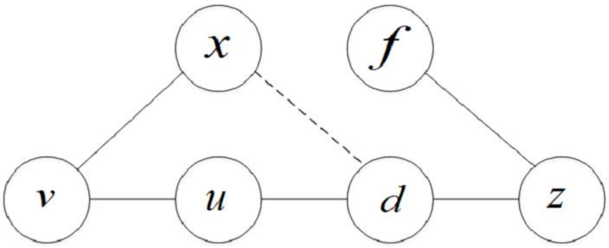

Fig. 3 Intrusion Detection

Consider Fig.3 where ADJ(v) = {x, u} and ADJ2 (v) = {d}. OLSR requires v to select u as its MPR so that ADJ2 (v) is covered. A malicious x, interested in being elected as a sole MPR of v, will claim that d ∈ ADJ(x). Since z ∈/ ADJ(x), but according to x's advertisement z ∈ ADJ2 (x), x should have appointed d ∈ ADJ(x) as an MPR for covering z. This cannot happen, indicating a contradiction

Where v must treat a HELLO message containing all nodes of the network except for ADJ (v), as a potential attack. Nodes must apply each of the mentioned rules sequentially, advancing from one rule to the next if there are no contradictions. Failure of any of the rules would require that v appoint x as a sole MPR only for the nodes that were exclusively declared in its HELLO message

Preventing the Intrusion Attack Using DIPS

The original DIPS were developed in order to identify and prevent the node isolation attack. In the black-hole attacks, however, this solution is incomplete. Attackers can still orchestrate their attack by dropping data packets that were to be routed through them – even when they were not appointed as sole MPRs.

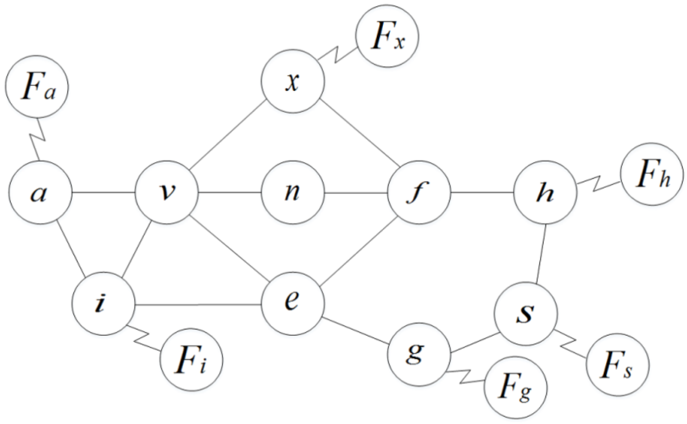

Fig. 4 Intrusion Detection and Prevention using DIPS

Avoidance of selecting a suspected node as a sole MPR, which is the crux of DIPS, mainly prevents the blackhole attack. There are, however, two additional venues in which a malicious node can circumvent DIPS based protection:

(1) When it is a natural candidate for passing data from ADJ2 (v) to v; and

(2) When topology restraints require that it be appointed as sole MPR, i.e., when there is no other connection to some node.

Our simulations show that although the probability of attack success is less in either of these attack venues when compared to the main venue, non-theless it is still feasible. Using internal knowledge gained by DIPS, we present an improved method denoted by IMP (short for IMProvement), as a method of further decreasing attack success to include these two venues as well.

To deal with these problems we propose using DIPS's contradiction rules to further influence routing decisions. Not only will we decide who should be in MPR0 (v), but other nodes in the network also make data routing decisions – on the fly – based on the previous outcomes of the rules. We call this improvement IMP, which can be summarized by Algorithm 1 in which k is a node on the optimal path between the source and destination nodes, and d ∈ ADJ2 (k) located further down the path.

.

Performance Metrics

We have used following performance metrics for evaluating effects of attack and effectiveness of our detection algorithm

Throughput

WIt is the ratio of the total number of bits transmitted (Btx) to the time required for this transmission, i.e. the difference of data transmission end time and start time (tstart). This metric depicts how the congestion control mechanism at the source node is affected by the packet losses caused by - nodes. A decrease in throughput is an outcome of any attack.

Throughput = $(B_{tx})/(t_{end} – t_{start})$ bps

Packet Delivery Ratio

This is defined as the ratio of the number of packets received at the destination and the number of packets sent by the source. Here, *pktd$_i$* is the number of packets received by the destination node in the ith application, and *pkts$_i$*is the number of packets sent by the source node in the ith application.

Average End-to-End Delay

It is average transmission delay of packets transmitted from source to destination. D is computed as the ratio of the sum of individual delay of each received data packet to the total number of data packets received. This metric is used to evaluate impact of a -attack on delay-sensitive applications of TCP-based MANETs. By intentionally discarding, delaying or reordering packets, a - node can increase the value of this metric; increase being caused by re-transmissions of such packets due to timeout at TCP source.

D= no.of received packed/total time

Result and Discussion

Our IoT adhoc network secnario scenario consists of 20-40 nodes configured with 'random-way point' mobility model. In our results, each point is average of ten simulation runs with different network parameters (topology and node mobility) using random seed values. In delay attack, the hold duration is randomly selected between 0.2 and 0.4 s for selected data packets over a specified fraction of time. In drop attack, the discarding period per second is chosen randomly between ranges of 0.02e0.04 s.

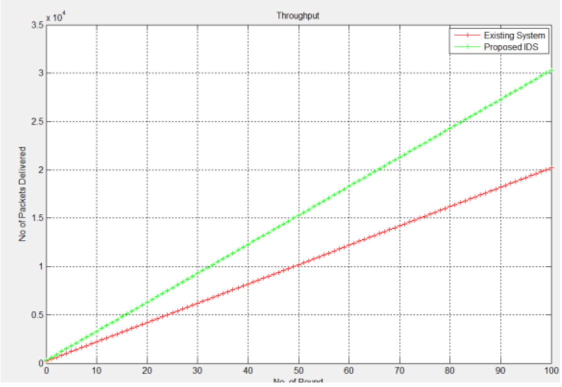

Fig. 5 Throughput

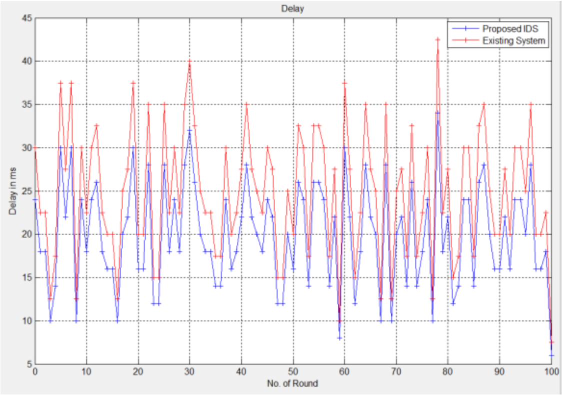

Fig. 6 Delay

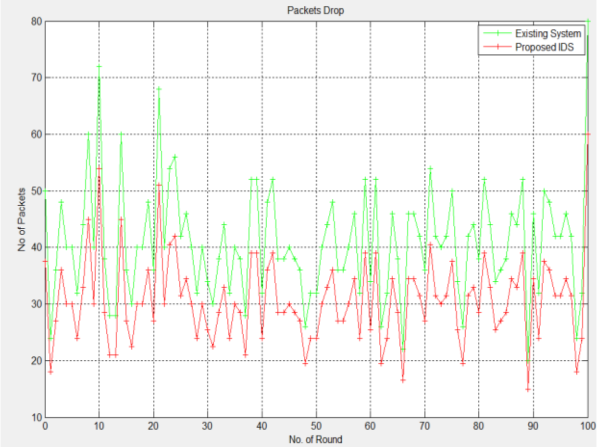

Fig. 7 Packet Drop

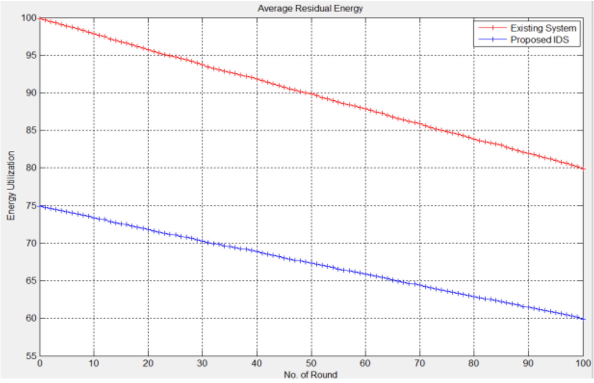

Fig 8. Average Residual Delay

Conclusion

Our IoT network scenario consists of 40 nodes configured with 'random-way point' mobility model (refer to Table 1 for mobility parameters). In our results, each point is average of ten simulation runs with different network parameters (topology and node mobility) using random seed values. Other simulation parameters along with their respective values used to create the target MANET scenario are listed in Table 1. In delay attack, the hold duration is randomly selected between 0.2 and 0.4 s for selected data packets over a specified fraction of time. In drop attack, the discarding period per second is chosen randomly between ranges of 0.02e0.04 s.

References

1. Ullah, Imtiaz, and Qusay H. Mahmoud. "Design and development of a deep learning-based model for anomaly detection in IoT networks." IEEE Access 9 (2021): 103906-103926.
2. Yin, Chunyong, Sun Zhang, Jin Wang, and Neal N. Xiong. "Anomaly detection based on convolutional recurrent autoencoder for IoT time series." IEEE Transactions on Systems, Man, and Cybernetics: Systems 52, no. 1 (2020): 112-122.
3. Tian, Zhihong, Chaochao Luo, Jing Qiu, Xiaojiang Du, and Mohsen Guizani. "A distributed deep learning system for web attack detection on edge devices." IEEE Transactions on Industrial Informatics 16, no. 3 (2019): 1963-1971.
4.] J. Toutouh, J. Garcia-Nieto, and E. Alba, "Intelligent olsr routing protocol optimization for vanets," IEEE Transactions on Vehicular

Technology, vol. 61, no. 4, pp. 1884–1894, May 2012.

5. [2] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on, Feb 1999, pp. 90– 100.
6. C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers," SIGCOMM Comput. Commun. Rev., vol. 24, no. 4, pp. 234–244, Oct. 1994. [Online]. Available: http://doi.acm.org/10.1145/190809.190336
7. T. Clausen, P. Jacquet, C. Adjih, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, and L. Viennot, "Optimized Link State Routing Protocol (OLSR)," 2003, network Working Group. [Online]. Available: https://hal.inria.fr/inria-00471712
8. D. Raffo, C. Adjih, T. Clausen, and P. Mühlethaler, "An advanced signature system for olsr," in Proceedings of the 2Nd ACM Workshop on Security of Ad Hoc and Sensor Networks, ser. SASN '04. New York, NY, USA: ACM, 2004, pp. 10–16. [Online]. Available: http://doi.acm.org/10.1145/1029102.1029106
9. C. Adjih, D. Raffo, and P. Mühlethaler, "Attacks against olsr: Distributed key management for security," in 2005 OLSR Interop and Workshop, 2005, pp. 28–29.
10. Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole attacks in wireless networks," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 370–380, Feb 2006.
11. C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, and D. Raffo, "Securing the olsr protocol," in Proceedings of Med-Hoc-Net, 2003, pp. 25–27.
12. E. Gerhards-Padilla, N. Aschenbruck, P. Martini, M. Jahnke, and J. Tolle, "Detecting black hole attacks in tactical manets using topology graphs," in 32nd IEEE Conference on Local Computer Networks (LCN 2007), Oct 2007, pp. 1043–1052.
13. B. Kannhavong, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour, "Nis01-2: A collusion attack against olsr-based mobile ad hoc networks," in IEEE Globecom 2006, Nov 2006, pp. 1–5.
14. W. Yu, Y. Sun, and K. J. R. Liu, "Hadof: defense against routing disruptions in mobile ad hoc networks," in Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies., vol. 2, March 2005, pp. 1252–1261 vol. 2.
15. M. Mohanapriya and I. Krishnamurthi, "Modified {DSR} protocol for detection and removal of selective black hole attack in {MANET}," Computers & Electrical Engineering, vol. 40, no. 2, pp. 530 – 538, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0045790613001596
16. R. H. Jhaveri, S. J. Patel, and D. C. Jinwala, "Dos attacks in mobile ad hoc networks: A survey," in 2012 Second International Conference on Advanced Computing Communication Technologies, Jan 2012, pp. 535–541.
17. S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. E. Nygard, "Prevention of cooperative black hole attack in wireless ad hoc networks." in International conference on wireless networks, vol. 2003, 2003.
18. S. Banerjee, "Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks," in proceedings of the world congress on engineering and computer science, 2008, pp. 22–24.