



Minimization of Gray-Hole Attack Effect for Secured Mobile Ad hoc Networks

Ms. M. Krishna Prasanna¹, Dr. M. Neelakantappa,
Assistant Professor, Associate Professor,
IT Department, BVRIT, Narsapur, TS

April 30, 2018

Abstract

Security is a main concern for any ad hoc network (like MANETs, VANETs, IOT etc.) as they are vulnerable to various kinds of attacks. Most of the popular protocols for detecting and mitigating the attacks, will process only after the commencements of attack. Instead of reactive measures, preventive measures are worthy, as they attempt to defend the attacks before it can happen to damage the performance of the network. However, both types of methods can be implemented either by collective effort of collaborative network nodes (i.e. built-in protocols added by security messages) or by internal evaluation of the attack state. This paper proposes a technique for minimising (reducing) the Gray-hole DOS attack. This technique does not assume any explicit-node collaboration and relies only on internal knowledge of each node achieved by regular routing information. This technique was tested through five different threat models with variable attacker capacities, which allows better realization of base of the attack as well as its prevention. The protocol is simulated in NS-3 simulator and the results demonstrate a reduction up to 55% in number of dropped packets, indicating great defence for Gray-hole attack on three MANETs as the MANETs application are evolving in a phenomenal way for the last two decades, they are emerging in the new technologies like VANETs and IOT as standalone network tool.

Key Words: MANETs, Gray-hole attack, DoS Attack, VANETs, IoT

1 Introduction

With the use of these MANETs the networking tools as well as the other emerging technologies like VANETs and IOT the securities on this underlying technologies have a huge demand which has been increased day-by-day. There are some of the ubiquitous MANET protocols like AODV[1], OLSR [2], DSDV [4] etc., which focus on the performance of data transfer and routing in an efficient manner. Thus it has lead to the protocols in which the current situations in which multitude of attacks are vulnerable which includes the worm-hole attacks, spoofing attacks, black-hole attacks, flooding attacks, replay attacks, colluding miserly attacks and many more.

The increase in use of MANETs, as a basis for technology like VANETs and IOT and as a standalone tool in networking, the demand of protection and security increases. However, ubiquitous MANETs were deployed focusing on data transfer performance and routing efficiently, not the issues on security. This, led to the present situation where the protocols are prone to numerous attacks, replay attacks, warm-hole attacks, black-hole attacks and many more.

The more general grey hole attacks and black hole attacks on MANETs are exhibited when a malicious node silently discards (some) gray hole or (all) black holes of the messages transmitting through it.-Gray hole is of higher sophistication and more devastating out of the two attacks as it discards messages selectively, making avoidance and detection difficult, performing anti black hole algorithms. Thus, gray-hole attack mitigation will solve the black hole attack also.

DCPM (Denial Contradictions with Pretended Node Mechanism) [5], is an algorithm designed to address a denial of service (DoS) specifically attack variant known as node isolation in OSLR protocols. DCPMs behaviour is its ability to mitigate the attack of node isolation by solely relying on knowledge acquired internally by each node during its routine routing in using the same technique used for attack to prevent the damage. As gray hole attacks and

both isolation require the same preliminary steps for execution of attack i.e, coaxing a victim for attacking as a MPR (Multi point relay), that is responsible for broadcasting a nodes existence to a network.

The structure of paper is as follows: In the Section 2.1 OSLR protocol is described, then the grey hole. In section 2.3, DCPM algorithm is presented briefly. Protection of OSLR MANET using DCPM, from grey hole is mentioned in section 3. The simulation model and the results achieved are in Section 4. Grey-hole attacks and OLSRs previous works have been discussed in 5th Section. 6th Section concludes and presents the future works.

2 BACKGROUND

2.1 Review of OSLR

The OSLR (Optimized Link State Routing Protocol) [2] is a routing protocol made for dense and large networks which is highly recommended for VANETs[6]. This optimizes the classic LSR protocol (Link State Routing), focused on reducing overhead network. While flooding propagation technique is used in the original LSR where a node receives any message must be transmitted to its neighbours. Re-transmission of selective messages is done by OSLR on a specific set of rules. Optimization is based on a subset of one-hop neighbours known as multipoint relays. Throughout the network, the controlling of packets is done by these forwarding agents.

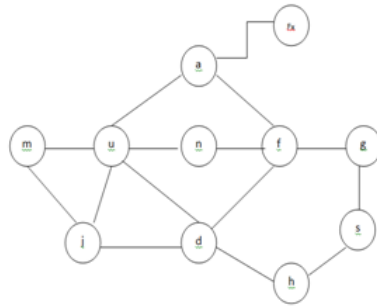


Fig. 1: Gray hole attack example: Node a claims of knowing all 2-hop neighbours of u, as well as nonexistent node Fs

A node selects MRPs as a subset of 1-hop neighbours, in such a way that MRPs allow the coverage of its all 2-hop neighbours. By decreasing the MRP selections, a node can transmit messages to all the 2 hop neighbours with least replication. Thus, both data packets and topology controlled messages are forwarded by these minimal MRP sets, allowing for least replicated messages still maintaining coverage network-wide.

Two-types of messages are used for the discovery of network topologies in OSLR: HELLO and TC (Topology control). The HELLO message declares a nodes knowledge of its surroundings, broadcasting to all its neighbouring nodes. Any node can hear the broadcasts and reply to the sender and is classified as one-hop neighbour. As a result, each node will acquire its local topology upto 2 hop ranges.

Additionally, OSLR needs all to be selected as MRPs periodically that advertises a TC messages list mentioning all nodes that chose the sender as MRP of it. The control messages are only transmitted through MPR super-network, decreasing network traffic in overall.

Based on both the HELLO and TC messages received, each node maintains a network topology in the network. For each discovered node, calculations are done and stored, the minimum hops required between source and destination (i.e. the shortest distance) between one of its destination nodes MRPs and itself.

2.2 Gray and Black hole Attack

Black holes here in the network refer to the locations where the malicious nodes remove the network traffic without notifying the source that the requested destination did not receive the packet. Nevertheless, every node on the transmitting path between destination and source is a black hole attacker. The surface of attack can be enhanced, with few steps specifically executed by the attacker in order to increase the probability of landing on the path of all victims or a specific victim. Our main concern, thus, with black holes, though not only a concern, is that when a node illegitimately coerces its topology so that it can be placed between a node and the victim, more than some random chances of such occurrences.

Black hole attack can be considered as a special case of gray hole attack, where selected packets are only dropped, while others

will be forwarded. This paper aims to reduce the effect of Gray hole attack, by considering the case of attacker, which selectively forwards packets of all nodes, except the victim node. At the same time, it will not isolate victim, as it passes the control packets.

An ad hoc network, running OLSR protocol is vulnerable to gray hole attack. The attacker, will send a dummy HELLO messages to its 1-hop neighbours, indicating it has more 1-hop nodes than it as in actual. Therefore there are more chances of choosing this node as a sole-MPR by its neighbours. This impact is greater, as more and more of its neighbours chooses this node.

Consider Figure1, illustrating a specific network architecture, in which a is an attacker-node, and u is a victim-node. The node a, sends its false HELLO message having 1-hop nodes f,u,h, where u and each of its 2-hop neighbours and adds a pretended-node Fx, so as to successfully attack the victim. As the node a seems to be most cost effective node of the entire network in us view, it selects a as its sole MPR. Thus attack can easily begins from here on, as most of the nodes of whole network will route their packets destined for u towards a, which will drop packets selectively.

2.3 Denial Contradictions with Pretended Node Mechanism

The DCPM protocol is proposed, to address the node-isolation problem of MANETs running the OLSR protocol. It detects the potential malicious nodes, which tries to send fake HELLO messages by use of internal information of the victim-node, without depending on any centralized or external information of the network topology. This early prediction prevents a possible massive attacks before it can commence. The DCPM protocol checks the validity of each HELLO message through contradictions between the claimed messages and its available network topology knowledge. In accordance to DCPM, sole MPR nominations are validated and allowed only when it does not lead any contradictions. In case of presence of contradictions, MPR will be nominated only for those 2-hop neighbour nodes for which the suspected node only is the access point. That means, it cant be nominated as MPR for other nodes for which alternative paths exist, which will greatly reduce the possible gray hole attack.

2.3.1 Notations

We used the following notation for illustrating the DCPM approach.

- S represents the set of all vertices(nodes) of the network
- $u \in S$, is representing victim-node of the attack in the network
- $a \in S$, is representing attacker-node of the attack in the network
- F_x represents the pretended node advertised by the node a
- $ADJC(u) \in S$ represents set of adjacent node (1-hop) set of u
- $ADJC2(u) \in S$ represents set of adjacent 2-hop node set of u
- $MPR(u) \in ADJC(u)$ represents the set of 1-hop adjacent nodes of u , who nominated u as their MPR and
- $MPR1(u) \in ADJC(u)$ represents the set of 1-hop adjacent nodes of u , who are nominated by u as MPRs

2.3.2 Contradiction Rules

DCPM protocol frames 3 rules, which have to be satisfied, by considering a HELLO-message sender as trust worthy node. These trusted nodes only are nominated as sole MPRs fro 2-hop nodes, which can be reached otherwise, following the OLSR protocol policy. **Rule-1:** Whenever node a advertises HELLO message, consisting of $ADJC(a)$, For each node $y \in ADJC(v) \cap ADJC(u)$, the node u should examine that $a \in ADJC(y)$.

This Rule1, can be easily illustrated through Figure 2, where $ADJC(u) = \{a, w, y\}$ and the node a is an attacking node. Node a advertises the HELLO-message, to claim that it knows the set of $ADJC2(u)$, consisting of y (as y is a us 2-hop neighbour via w). But $y \in ADJC(z)$ and since y is not included a in its HELLO-message, u will suspects a as malicious node (attacker).

Rule-2:

For every node z , represented in HELLO-message, the node u have to verify, whether there exists any node y , i.e. $y \in ADJC(z)$, such that

- (i) $y \notin ADJC(a)$; therefore, not represented in as HELLO-message and
- (ii) $z \in ADJC2(u)$; therefore z is located at least 3-hops away from u .

Once (i) and (ii) conditions are verified, condition must be checked if a is appointed $t \in \text{ADJC}(a)$ as MPR for covering y .

As shown in Figure 3, in which, $\text{ADJC}(u) = \{a, w\}$ and $\text{ADJC2}(u) = \{e\}$, the Optimized Link State Routing (OLSR) protocol needs u to choose w as its MPR, such that $\text{ADJC}(w)$ is covered. A malicious node a shows interest to be elected as a sole MPR of u , can claim that $e \in \text{ADJC}(a)$. As $y \notin \text{ADJC}(a)$, a should have nominated $e \in \text{ADJC}(a)$ as MPR for covering y . This could not happen, showing a contradiction.

Rule-3:

Node u must treat a HELLO-message, consisting all nodes of the network except for $\text{ADJC}(u)$, as a potential attack.

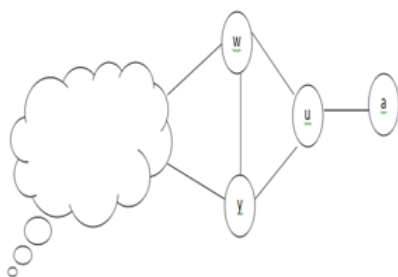


Fig. 2. Sample Node-Topology to Identify Contradictions

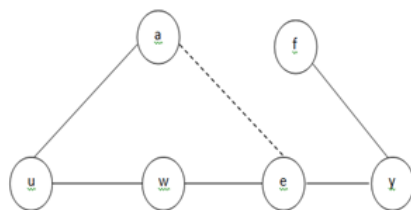


Fig. 3. Node a attacks u , by advertising a nonexistence link (a,e)

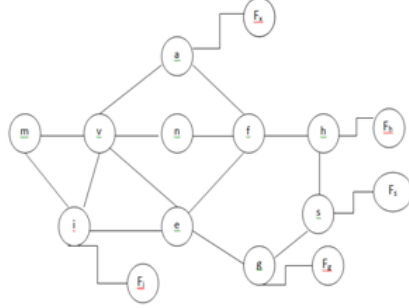


Fig. 4: Expansion of Network in Fig.1, with DCPM Protection

The nodes b, j, h, t, i represent the frictions nodes of DCPM. No MPR is nominated by y for covering $\{t, f_h\} \in \text{ADJ}(h)$ despite y's false claim which shows that $h \in \text{ADJ}(y)$; therefore, $\{t, f_h\} \in \text{ADJ}_2(y)$. Applying DCPM rules attack y's malicious intent is identified by w and stops from nominating y as the sole MPR. Therefore, $\text{MPR}(w) = \{b, j, y, f\}$. Although $\text{ADJ}(y) = \{w, g, h, f_b, f_j, f_y\}$, or it claims, $\text{MPR}(w) - \{y\} \neq \Phi$, whereas others are appointed into $\text{MPR}(w)$. Significantly, $y \in \text{MPR}(w)$, despite suspecting it. This is needed for accessing $\{f_y\}$ the group of nodes known completely by y and is also essential for initialization of MANETs and forward evolution.

3 PREVENTION OF GRAY-HOLE ATTACK BY USING DCPM

Denial contradictions with frictions node mechanism was developed for the identification and the prevention of the isolation attack of node. This is an incomplete solution for the attacks of Gray-hole. Attacks are still planned by the attackers by dropping the data packets which should be routed, even if they didn't act as the sole MPRs.

The main aspect of DCPM is to avoid the selection of the suspected node as the sole MPR which prevents a Gray-hole attack. There are two more venues how the malicious node avoids DCPM formed protection. Augmenting DCPM along with IMP for preventing Gray-hole attack might not increase network overhead of

what was discussed [16] for DCPM, we can claim that there is negligible networking cost of IMP.

ALGORITHM: 1.1 IMP

```

IMP (l, e)
S ← (ADJ (l) ∩ ADJ (e))
for (every y ∈ S) do
mark y as suspect
if (y) is marked as legitimate
return (y)
else
S ← S - {y}

```

In fig 2, apart from w g also suspects y as malicious. In g's view of network, y's HELLO message includes a contradiction. Y is showcasing that $ADJ(w) = \{w, g, h, f_b, f_j, f_y\}$.

However rule 2 proves g that y is lying but h isn't in the neighbourhood of y. g will hold back from routing the data through y if any other acceptable option exists. Nodes might route the data along suspicious nodes. Simulation has found that there might be some cases where this route choosing mechanism increased the delivery of packets in number by 20% more than what is achieved by using DCPM without extra cost.

Now y attains apposition for attacking w in spite of DCPM's protection with the help of supplemental attacks mentioned above. Assume for the topology shown in the figure 2 where I transmits one message to w. As the shortest path is through g, I delivers the received message to g. As $g \in ADJ_2(w)$, it can choose any of the paths going through y, m, f irrespective to the appointment of MPR for w. The probability of packets travelling along the attacker to the victim is high. Contraction rules of DCPM are proposed to handle such problems. Routing decisions are influenced using them.

Decision of choosing MPR (w) and other nodes that make decision for data routing are made using previous outcomes of these rules. This can be called as an improvement IMP that can be reviewed by algorithm 1.1 in which l destination nodes and e $ADJ_2(l)$ residing along the path.

4 EVALUATION

As the network topologies are countless, expected result estimates have to be achieved by simulation. In the following section, we illustrate varying simulations, which were processed, so as to justify the usage of IMP to present Gray hole attacks.

4.1 Simulation

In the network simulator NS-3[6], we used the existing OLSR protocol for our simulation. This was modified to execute our DFCM protocol, according to the procedure as described above each simulation in set to run 500 times and average of the reported result were taken for evaluation. The speed of the nodes in the MANET is set to the range 1.0 to 2.5mts/sec and the transmission range is set to 300mts. For testing effectiveness of our DFCM protocol in defending, Gray hole attacks. Hence, random network topology was chosen, with variation in the number of nodes with network density range from 20 to 100 nodes over an area 500m*1000mts. The case of network simulation, without connectivity among the nodes was not considered, as it doesn't represent the real time scenario. Hence, this case will not account in the computed outcome.

At each step of simulation, 3 pre-defined nodes are used as a source node, an attacker and a victim, the source node represents the messages for sending to the destination node. The source node and victims are randomly placed. But, it requires that there must be at least 2-hop distance between source node and victim. Hence, all the cases which do satisfy this condition are discarded. The justification for this condition is on the bases of the fact that, the source node and the victim which are 1-hop neighbour will be implicitly protected from malicious nodes which avoids the need for the other protection strategies. The attacker node is designed in one of the 5 various capacities as presented below:

- **Passive-Silent-Attacker (PAS):** Passive silent attacker will be placed in the network randomly. It will not increase its chances for becoming a routing node to forward the packet. This PSA attacker type results can be used as bench mark for the gray hole attack, in comparison with other sophisticated attacker.

- **Randomly-Located-Attacker (RLA):** In similarity with

PSA attacker, this node also will be placed in the network randomly. The main difference is it will try to get itself chosen as a sole-MPR for the victim node, in case theses are 1-hop neighbor to it.

- **Initially 1-Hop Neighbor-Attacker (IHNA):** This attacker will be located as a 1-Hop neighbor to the victim initially. 1-HNA attacker is similar to the one above (RLA), except that its initial position is not random, instead it must be 1-Hop neighbor to the victim node.

- **Shadow Attacker (SHA):** This SHA attacker has a capacity to shadow the victims mobility from the distance of 200mts, by moving along with it by maintaining 1-hop distance constantly. This is the main difference, when compared to the above attacker, who starts as a neighbor, but the distance will vary during the simulation.

- **MITM-Attacker:** This attacker enhances the capacity of the shadow attacker. Apart from being 1-hop neighbor throughout the simulation, it gets awareness of the location of the source node. This allows it, to adjust for locator itself in-between these two nodes, so that it maintains to be on the shortest path in between them. Thus it increases chances of being attacker during the packet transfer between them.

For each type of this attacker, we evaluated the following cases:

- **Arrived:** The package (the set of packets in a transmission session) is arrived at destination.
- **Last-by-3party:** This package was last by 3 party in its way due to certain cause, without regard to the attacker.
- **Attacker-Neighbor:** The given package was dropped by the attacker who is the 1-hop neighbor to the victim, even though, there will be another node, who can forward the same packet.
- **Attacker-Single-neighbor:** The given package was dropped by this attacker (either accidently or intentionally), where there was only one route available means through this attacker node. Hence in this case, there is no chance of packet regarding to the destination.
- **Attacker:** The given package is dropped by that attacker, who located at least 2-hop distance from the victim-node.

We observed that "Attacker-Neighbour", will mainly be influenced by IMP. "Last-by-3party" and Attacker", cannot be influenced beyond certain random and independent change, there is no noticeable improvement for "Attacker-Single-Neighbour", as IMP will not be able to change the network topology, instead it can

wisely select party between equivalent-party. In case if path only exists to the victim, then there will be no alternate options, which can circumvent this attacker for IMP for selection.

Every simulation was executed, 1) without any attacker, 2) under-attack without any protection, 3) under-attack with DCPM protection and, 4) under-attack with IMP protection.

4.2 RESULTS

As indicated in the Figure 5 and 6, the percentage of dropped packets will be reduced with the increase in population density in a network simulation for both cases of with movement (M) and without movement (NM) respectively.

In each of these graphs, the X-axis indicates the density of the network, in terms of number of nodes in the random network environment from 20 to 120. Whereas the Y-axis indicates the percentage of delivered packets in each of the case.

In both the graphs, the attackers success is high, for the lowest population density (40%). Also, as we expected, the MITM attacker is the most effective (strongest) whereas the PSV attacker is the least effective (weakest) among all the potential attackers.

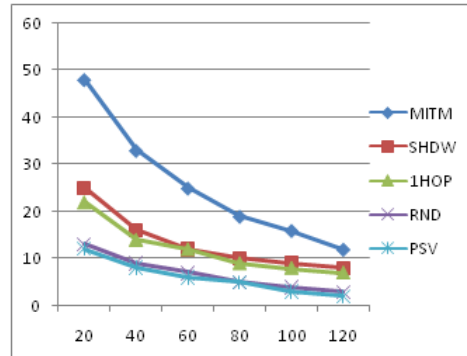


Fig. 5: %Drop packets(M)

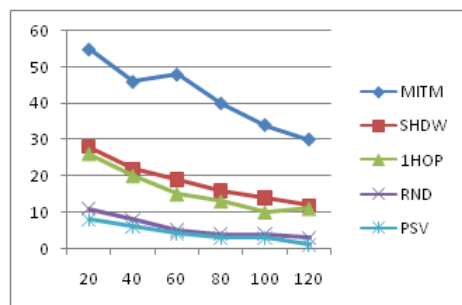


Fig. 6: %Drop packets (NM)

To improve the attack delivery ratio, under various types of attackers, we deployed IDCPM which is the improvement version of DCPM. With the results of the simulator, it is evident that, even at low damage cases of the attacker, IDCPM improves the number of packets delivered successfully by minimizing the damage caused by the attacker. In addition for dense network, IDCPM impact will be high. Figures 7,8,9, and 10 shows the percentage of delivered packets under attack (UA) and without attack (NA), with attack under the protection of DCPM and with attack under protection of IDCPM with movement (M) and without movement (NM) of the propagating nodes at every attacker groups.

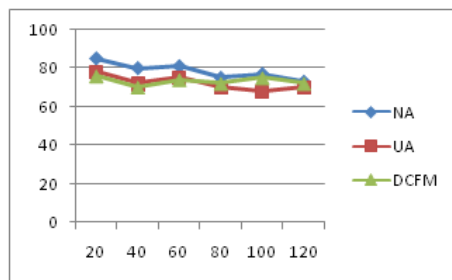


Fig. 7: % of delivered packets PSV Attacker (M)

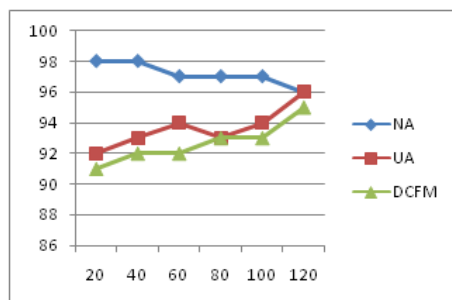


Fig. 8: % of delivered packets PSV Attacker (NM)

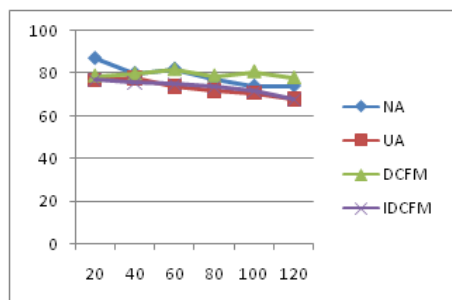


Fig. 9: % of delivered packets RND Attacker (M)

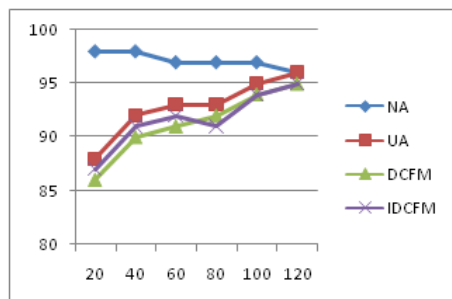


Fig. 10: % of delivered packets RND Attacker (NM)

5 CONCLUSION

This paper illustrates the improved version of OLSR algorithm for mobile networks such as MANETS, VANETS, IOT etc for defending gray hole and black hole attacks. By observing and getting the

information by participating nodes, we have decreased the captured packets by a significant factor which is highly compared to existing conventional DCPM technique under similar conditions. In all the cases of the simulation, we assumed that (which is practical in most of the real situations) an active attacker will try to influence the network topology maliciously for increasing the attack surface.

Even though, the potential attackers which are undetected can also drop packets, we designed IDCPM in such a way that, in most of the cases the number of routes passing through than is greatly reduced, which decreases the possibility of attacks.

In future work, we have to redesign IDCPM with minor adjustments in such a way that it can work for the vehicular Ad hoc networks as well.

References

- [1] Goldsmith.A, Effros.M, Koetter.R, Medard.M, Ozdaglar. A, and Zheng.L, Beyond-Shannon: the quest for fundamental performance limits of MANETs, published at IEEE Communication in May-2011.
- [2] Zhang.J, Chen.J, and Sun.Y, Transmission power adjustment of wireless-sensor network using fuzzy control alg. International Conference: Wireless Communication Mobile Computing, in June-2009.
- [3] Grosclauser.M and Tse.D.N, Mobility increases the capacity of ad-hoc wireless-networks publication in INFOCOM in Year2001.
- [4] Gamal.A.E, Maman.J, Prabhakar.B and Shah.D, Optimum throughput delay scaling in MANETs: part-I: the fluid-model, at IEEE Transaction Information Theory., in June-2006.
- [5] Shila.D.M and Chang.Y, Ad-hoc wireless-networks meeting the infrastructure:- mobility, delay and capacity, publication in INFOCOM in Year2002.
- [6] J. Toutouh, J. Garcia-Nieto, and E. Alba, Intelligent OLSR routing protocol optimization for VANETs, IEEE Trans. Veh. Technol., vol. 61, no. 4, pp. 1884 1894, May 2012.

- [7] C. E. Perkins and E. M. Royer, Ad-hoc on-demand distance vector routing, in Proc. 2nd IEEE Workshop Mobile Comput. Syst. Appl., Feb. 1999, pp. 90100.
- [8] NS-3 Consortium, The ns-3 network simulator. (2016, Jan.). [Online]. Available: <https://www.nsnam.org/>
- [9] T. Poongodi and M. Karthikeyan, Localized secure routing architecture against cooperative black hole attack in mobile ad hoc networks, *Wireless Personal Commun.*, vol. 90, no. 2, pp. 10391050, 2016. [Online]. Available: <http://dx.doi.org/10.1007/s11277016-3318-5>
- [10] S. Djahel, F. Nait-Abdesselam, and A. Khokhar, An acknowledgment- based scheme to defend against cooperative black hole attacks in optimized link state routing protocol, in Proc. IEEE Int.Conf. Commun., May 2008, pp. 27802785.
- [11] M. S. Khan, Q. K. Jadoon, and M. I. Khan, A comparative performance analysis of MANET routing protocols under security attacks, in *Mobile Wireless Technol.*, Berlin, Germany: Springer, 2015, pp. 137145. [Online]. Available: http://dx.doi.org/10.1007/9783-662-47669-7_16
- [12] J. M. Chang, P. C. Tsou, I. Woungang, H. C. Chao, and C. F. Lai, Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach, *IEEE Syst. J.*, vol. 9, no. 1, pp. 6575, Mar. 2015.
- [13] R. H. Jhaveri and N. M. Patel, A sequence number based bait detection scheme to thwart grayhole attack in mobile Ad Hoc networks, *Wireless Netw.*, vol. 21, no. 8, pp. 27812798, 2015. [Online]. Available: <http://dx.doi.org/10.1007/s11276015-0945-9>
- [14] A. D. Patel and K. Chawda, Dual Security Against Grayhole Attack in MANETs. New Delhi, India: Springer, 2015, pp. 3337. [Online]. Available: <http://dx.doi.org/10.1007/97881-322-2009-1>
- [15] M.-Y. Su, Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems,

Comput. Commun., vol. 34, no. 1, pp. 107117, 2011.[Online].Available:[http:// www.sciencedirect.com/ science/ article/ pii/ S0140366410003774](http://www.sciencedirect.com/science/article/pii/S0140366410003774)