Link Stability Based Secure Path Selection Scheme for Manet

T.Sophiya, MCA.,M.Phil.,
Assistant Professor, Department of Computer Science
Morappur Kongu College of Arts & Science

OPEN ACCESS

Volume : 6

Special Issue : 1

Month : September

Year: 2018

ISSN: 2321-788X

Impact Factor: 3.025

Citation:
Sophiya, T. (2018). Link Stability Based Secure Path Selection Scheme for Manet. *Shanlax International Journal of Arts, Science and Humanities*, 6(S1), pp.6–17.

DOI:
https://doi.org/10.5281/zenodo.1410945

Abstract

A mobile ad hoc network is a collection of wireless nodes that can dynamically be set up anywhere and anytime without using any pre-existing network infrastructure.The Lot of work is proposed based upon Secure Path Selection Scheme algorithm. While working on Secure Path Selection Scheme algorithm, Direct Trust Calculation was used in which zero while be discarded and one will be selected and which become a best path to send packet from source to destination. Direct trust calculation also identify the two attackers namely- Black hole attackers and gray hole attackers The role of Black hole attackers is to drop all the data packet and send false route reply whereas the role of gray hole attackers is to selectively drop the packet and send false route reply The main role of Secure Path Selection Scheme is to identify and remove attackers path and select a genuine path to send data packet to the sender. In Link Stability Secure Path Selection Scheme the selective trust value one those are having high speed will be dropped while the low speed value will be selected for stable path for sending packet from source to destination The Simulation results shows the improvement of better results using performance metrics such as Packet Delivery Ratio, Throughput and Routing Overhead.

Keywords: Mobile ad hoc network, Black hole attack, Gray hole attack,Link stability based secure path selection scheme.

Introduction

An Ad hoc network is a collection of mobile nodes, which forms a temporary network without the aid of centralized administration or standard support devices regularly available as conventional networks [1]. These nodes generally have a limited transmission range and, so, each node seeks the assistance of its neighboring nodes in forwarding packets and hence the nodes in an Ad hoc network can act as both routers and hosts. Thus a node may forward packets between other nodes as well as run user applications. By nature these types of networks are suitable for situations where either no fixed infrastructure exists or deploying network is not possible. Ad hoc mobile networks have found many applications in various fields like military, emergency, conferencing and sensor networks. Each of these application areas has their specific requirements for routing protocols. Limitations of MANETs: They provide access to information and services regardless of geographic position. These networks can be set up at any place and time. Independence from central network administration. Self-configuring network, nodes are also act as routers. Self-configuring network, nodes are also act as

routers. Less expensive as compared to wired network. Scalable-accommodates the addition of more nodes.Improved Flexibility.Robust due to decentralize administration. The routing protocols for ad hoc wireless networks can be broadly classified into four categories based on Routing information update mechanism,Use of temporal information for routing, Routing Topology, Utilization of specific resources. These are good for networks which have less node mobility or where nodes transmit data frequently. DSDV (destination sequenced distance-vector), WRP (wireless routing protocol), CGSR (cluster-head gateway switch routing protocol) and STAR (source-tree adaptive routing protocol) are some examples of table-driven routing protocols.

Reactive routing protocols are on-demand routing protocols. In which nodes do not contain complete information of the network topology, for the reason that it changes constantly. Path finding process and information exchange process execute when any node requires a path to communicate with the target node. Some examples of reactive routing protocols are: ABR (Associativity-Based Routing), AODV (Ad Hoc On-Demand Distance-Vector), LAR (Location-Aided Routing), DSR (Dynamic Source Routing) and. For our simulation using AODV routing protocol.

Related Works

The working in routing algorithm of MANET is still very challenging problem in the computer science researchers. Due to its nature, providing a quality of service depends on the selection of route and its protocol. The lot of researchers are propose different algorithm to have a secure path protocol in order to provide the QoS in MANET Environment.

Marti, S., Giuli, T. J., Lai, K., and Baker, M. [3] Marti et al. have proposed the watchdog system to detect malicious nodes in MANET. In watchdog system nodes use promiscuous hearing technique, in which, neighbor nodes promiscuously hear sender node transmission. If packet drop observed, it increases failure counter of sender node. If failure counter exceeds threshold then sender node reported as malicious node.

Liu, K., Deng, J., Varshney, P. K., and Balakrishnan, K. [4] Liu et al. have proposed the TWOACK system. System runs on a group of three consecutive nodes. In which, first node sends data packet to third node through middle node. If third node receives a data packet, it sends an acknowledgment packet (TWOACK) back to first node. If first node receives TWOACK packet, then transmission is successful. Otherwise, malicious behavior of node is reported. Among three consecutive nodes 1–3, node 1 sends packet to node 2, node 2 forward it to node 3. Node 3 sends TWOACK packet to node 2. Node 2 further forwards TWOACK packet to node 1.

Sheltami, T., Al-Roubaiey, A., Shakshuki, E., and Mahmoud, A. [5] Sheltami et al. have proposed the adaptive acknowledgement (AACK) system. Source node sends data packet to destination node. If source node receives an acknowl-edgment packet from destination node, it indicates the successful transmission. Otherwise, source node switches to TWOACK mode to detect malicious nodes. source node 0 sends data packets to destination node 4. After receiving the data packet, node 4 sends an acknowledgment (ACK) packet. If node 0 receives ACK packet of node 4 from node 1, it indicates successful transmission.

Link Stability based Secure Path Selection Scheme for Manet

The main concentrating of this analysis is to handle secure path selection in MANET using the secure path selection scheme technique. The node is evaluated based on their behavior. Once the attacks are detected, then delegate node receives the join request during, the data transmission each node in the trusted path checks whether the next node in the path are capable of receiving and forwarding the packets. If a node successfully receiving and forwarding the packet to the next node then transmission continues [11]. The following assumptions are considered to identify the secure path in AODV protocol,

Overview

1. For all communications source node is not malicious
2. Address of all delegate nodes is already known to legitimate nodes
3. Delegate nodes update and broadcast trusted nodes list in network
4. System will handle only black hole attacks and gray hole attacks

Attackers in the Environment

Mobile ad hoc network (MANET) is self-configuring open medium network. MANET nodes act as both host as well as router and cooperate with each other to form a network without any centralized control. Nodes also have random mobility and this makes network topology dynamic. Easy deployment and less configurations makes MANET more usable in military and disaster recovery operations. But, these features bring serious security attacks in MANET, such as black hole and Gray hole attacks.

Black Hole Attacks

MANET more usable in military and disaster recovery operations but these features bring a packet drop attack or black hole attack is a type of denial-of-service attack accomplished by dropping packets. Black holes refer to places in the network where incoming traffic is silently "dropped", without informing the source that the data did not reach its intended recipients shows the black hole attack. Black Hole attacks effects the packet delivery and to reduce the routing information available to the other node [12] [13]. the black hole attack has two properties. First property is, the node exploits the MANET protocol, such as AODV (Ad hoc On-demand Distance Vector) to advertise it as having a valid path to a destination node, even though the path is invalid, with the intention of intercepting packets. Second property is the attacker consumes the intercepted packets without forwarding to any other node.

Secure Path Selection Scheme

The Secure path Selection Scheme algorithm mainly consist of attacks detection and send request and response for secure path and link stability path using a Trust initialization,Attack Scenario Creation, Trust Initialization, Secure Path Selection and Link Stability Based Secure Path Establishment, Performance Evaluation

Algorithm for Link Stability Secure Path Selection Scheme

D ← D1,D2,.. Delegate nodes
N ← N1,...,Nn Nodes in the network
T ← Trusted nodes list
Phase 1: Trust Initialization
For N= N1 to Nn do
N(i) sends join request with trust value to D
if Trust value N(i) is 1: yes then
Accepts join request and add N(i) in T
else
Rejects join request
end
D broadcast T in network
T get deployed in network
Phase 2: Secure path selection
loop 1: Source broadcast RREQ

if Source or intermediate node receives RREP: Yes then
if RREP from node listed in T: Yes then
Accepts RREP
Source sends data packets through established secure path
else
Discards RREP
goto loop 1
end
Phase 3: Link Stability Based Secure Path Establishment
For less mobility do
else
goto loop 1
end

Direct Trust Calculation

The mobile nodes while communicating with other nodes the direct trust value of all the communicating nodes are calculated and stored in the trust table of corresponding node with field name using index of node, direct trust value and one more total trust value of the corresponding mobile node and otherwise by default all the mobile nodes while communicating with other mobile nodes, the direct trust value of all of the communicating nodes are calculated and stored in the trust table of corresponding node After some time the neighbor's nodes may move out of the range of a particular node due to their mobility and again they come back to the transmission range then again trust value is calculated and the corresponding entry in the table is updated.

DTxy = Ps/PR
DTxy =the final direct trust value of x and y.
Ps= the successful packet sent from the node x.
PR = the successful packet receive from the node y.

Direct Trust – Based Detection

Step 1: Packet sent from the node x.
Step 2: Packet receive from the node y
Step 3: It generates a report and validate the report rules.
Here, generate a report using Direct Trust (DT) calculation.
Step 6: The Final Trust value is retrieved.
if (final trust < 1)
{
If (attacks is detected)
Black hole attacks drop all the packet;
Gray hole attacks selectively drop the packet;
else
Transfer false route reply;
}
Step 7: Finally, the performance is evaluated.

Table 5 Black Hole Attack Trust Table

Node	Trust Value
1	1.000000
2	1.000000
3	1.000000
4	1.000000
29	0.000000

Data Transmission Via Black hole Attacker

In Transmission History, source node 24 transfer the data to destination through black hole 29. If the attacker is black hole node, drops the packet. Due to the data transmission, thetrust value is calculated by ratio between the no of packets are received to the no of packets are forwarded. The misbehavior of attacker node trust value is decreased.

Table 6 Transmission History

Node	Forward Count	Received Count	Trust
29	0	1	0.000000
29	0	2	0.000000
29	0	3	0.000000
29	0	4	0.000000

Black hole Attacker-29 drops the packet source node 24 broadcasts the RREQ request packet towards the destination node. When attacker node 29 receives the RREQ packet, it sends false RREP(Route Reply to Source node). Therefore source node select the shortest path as attacker path and sends data to attacker Path.

Attacker Node (Black hole or Gray hole) Sends False Route Reply in Trace file

S 1.001308306 _17_ RTR --- 0 AODV 44 [0 0 0 0] ------- [11:255 22:255 30 22] [0x4 1 [17 **2147483600]** 10.000000] (REPLY)

Attacker drops the packet (shown in trace file)

D 2.005421047 _11_ RTR LOOP 10 cbr 520 [13a b 16 800] ------- [22:0 17:0 29 11] [10] 1 0

Gray Hole Attacks

The gray hole attack is known as variants of black hole attack, in which, a malicious node sends false RREP packet to source node. Malicious node then selectively drops data packets. So, the performance and security of network degrades. The security solutions for MANET are classified into two main types: prevention and detection [14]. Prevention technique such as encryption is expensive for MANET [15]. It consumes constrain resources. However, encryption techniques cannot prevent all attacks. In detection solution, the intrusion detection system is essential which detects attackers. [16] [17] One of the major issue about the gray hole attacks is that it misguides the source b*y advertising that there is a valid and shortest path to the destination. Thus the malicious node could do harm the network by degrading the network performance, disturbing route discover process etc. In direct trust calculation comes under direct observation of neighbor's one hop to

another .In every mobile node in the network monitors the behavior of its neighbor's node, and if any abnormal activity is detected, to evaluate trust value. In this module to monitors the neighbor's nodes by trustable listening to their communication for detecting dropped, delayed, and forwarded packet. In every mobile node in the network monitors the behavior of every other neighbor's node really forwards the packet or drop and send false route reply [18].

Table 7 Gray Hole Attack Trust Table

Node	Trust Value
1	1.000000
2	1.000000
3	1.000000
29	0.312000

In Transmission History, source node 24 transfer the data to destination through grayhole node 29. If the attacker grayhole that selectively drops the packet and send false route reply. Due to the data transmission, the trust value is calculated by ratio between the no of packets are received to the no of packets are forwarded. The misbehavior of attacker node trust value is decreased.

Table 8 Transmission History

Node	Forward Count	Received Count	Trust
29	0	1	0.000
29	1	2	0.500
29	2	3	0.666

GrayHole Attacker-29 drops the packet.

Join Request

Each node sends join request to Delegate node 0. Delegate node 0 checks the trust value of that node, If the trust value is maximum, then node will be added into trusted List. After receiving trust value, sends acknowledge packets to join reqSuested nodes.

Legitimate Nodes-36 sends join request with trust=1 to Delegate node=0
Legitimate Nodes-37 sends join request with trust=1 to Delegate node=0
Legitimate Nodes-38 sends join request with trust=1 to Delegate node=0
Legitimate Nodes-39 sends join request with trust=1 to Delegate node=0
Then Delegate node 0 broadcasts the trusted node list to entire network.

Data Transmission Based Secure Path Selection

Now source node 24 sends data to destination 17. But during Route discovery process, the attacker node 29 sends false route reply to source node 24. To identity and remove this attacker path and select a genuine path , the proposed secure path selection scheme, when node receives the RREP packet, it checks that node in trusted list. If I t is not in trusted list, drops the RREP packet. Otherwise accept the RREP packet [19] [20] [21].

For instance

AT THAT Tim e- 16.0009 Black Hole and Gray hole Attacker-17 sends false Route Reply

Node-37 is received RREP Packet from Node-29
Discards this packet
Now secure path is established through genuine path.
Path->24-1-17

1.4 Link stability Based Secure Path Selection

In Secure Path selection scheme the attacker node is detected and data transfer through the genuine path. But it suffers from the Link breakage. To solve this issue, the link stability based Secure Path Selection Scheme the forward node selection is based on the high stable node. A link stability is measured based on the node speed those ate having high speed will be dropped while the low speed value will be selected for stable path [22].

For instance,

Data Routing index-24 nexthop=29 saddr=24 daddr=17 seqno=207 hopcount=1 pktsize=1020
Current Node--24 Neighbor---1----Speed--14
Current Node--24 Neighbor---21----Speed--49
Current Node--24 Neighbor---17----Speed--35
Current Node--24 Neighbor---14----Speed--41
Current Node--24 Neighbor---10----Speed--25
Current Node--24 Neighbor---29----Speed--42
Current Node--24 Neighbor---3----Speed--45
Highly Stable Alternative Nexthop for node 24 is-1
High Stable Path=> 24-1-17

Table 9 Simulation Parameter

Simulator	**Network Simulator 2.35**
Number Of Nodes	40
Area	600m x 600m
Packet Size	512 bytes
Mac Type	802.11
Queue Length	50 Packets
Antenna Type	Omni Antenna
Propagation Type	TwoRayGround
Routing Protocol	AODV
Simulation Time	50seconds

Experimental Results and Analysis

Simulation Environment

The performance of future SPSS is evaluated against LSSPSS system using the network simulator (NS2) under black hole attack and gray hole attack. NS2 is a discrete event simulator targeted at networking research. NS2 provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless networks. The antenna used is an Omni directional

antenna which radiates radio wave power uniformly in all directions in one plane, with radiated power decreasing with elevation angle above and below the plane, dropping to zero on antenna's axis. The propagation model use d as two ray ground. The two ray ground reflection model considers both direct path and a ground reflection path. The routing protocol used is ad hoc on demand distance vector (AODV). [23] [24] [25]. The MAC type is 802.11. The simulation is run for node 40, 45, 50, 55 and 60 . The 40 mobile nodes are deployed in 600m x 600m environment size

For each set of parameters chosen for the simulation, multiple runs of the simulator are executed varying the initial position pairs that communicate at a node An average of the values got in the multiple runs is then calculated to the final results. Simulation result shown in the below figures.

Performance Metrics

To correspond to the special distinctness and recital of network following metrics are used in our simulation:

Packet Delivery Ratio

Packet delivery ratio is the ratio of packets that are successfully delivered to a destination compared to the number of packets that haves been sent by sender

In order to calculate packet delivery ratio we need total number of packets sent and number of received packets

$$PDR = \frac{\text{Number of packet received}}{\text{Number of packet transmitted}} X\ 100$$

Where,

Pr is total packets received and

P s is the total packets sent.

Routing Overhead

Routing Overhead to check whether the neighbor node is active Both, routing and data packets have to share the same network bandwidth most of the tines, and hence, routing packets are considered to be and overhead in the network. This overhead is called routing overhead.

Throughput

Throughput is the number of successfully received packets in a unit time and it is represented in bps. Throughput is calculated using awk script which processes the trace file and produces the result.

Throughput = Pr / (T2-T1)

Where,

Pr is total data size received,

T1 is the start time and

T2 is the stop time

Result and Analysis

Packet Delivery Ratio

The packet delivery ratio of proposed Link Stability Secure Path Selection Scheme protocol is

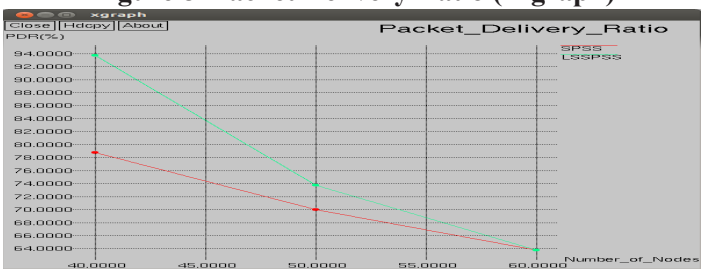
better than than Secure Path Selection Scheme.

Due to data transmission, the Link Stability Secure Path Selection Scheme protocol selects high stable next hop in which reduces the link breakage probability and improves data delivery performance.

Table 10 Packet Delivery Ratio for Secure Path Selection Scheme and Link Stability

Node	Routing Overhead for SPSS	Routing Overhead for LSSPSS
40	3.037	3.259
50	4.650	4.881
60	6.312	6.436

Figure 8 Packet Delivery Ratio (X graph)



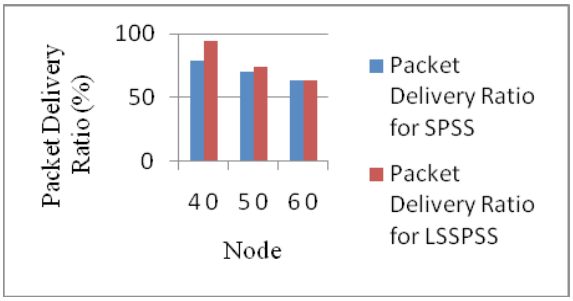


Figure 10 Packet Delivery Ratio(chart)

Routing Overhead

Overhead of LSSPSS is increased than the SPSS. Because due to stable route selection, if it is not route to the destination, it reinitiates the route discovery process. Thus it increases the routing overhead.

Table 11 Routing Overhead for Secure Path Selection Scheme and Link Stability

Node	Number of Packet Transmitted	Packet Delivery Ratio for SPSS	Packet Delivery Ratio for LSSPSS
4 0	80	78.75 %	93.76%
5 0	80	70%	73.75%
6 0	80	63.75 %	63.75%

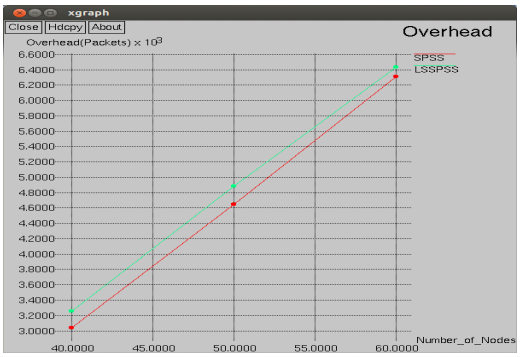


Figure 11 Routing Overhead (X Graph)

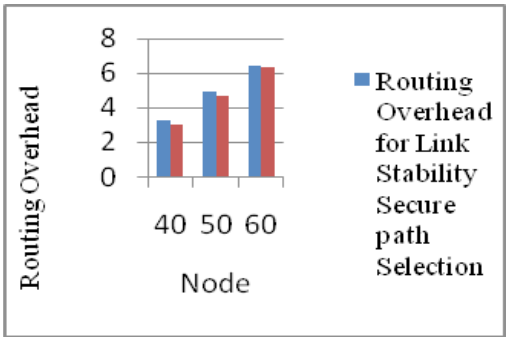


Figure 12 Routing Overhead (Chart)

Throughput

Throughput of proposed LSSPSS protocol is better than than SPSS. Due to data transmission, the LSSPSS protocol selects high stable next hop in which reduces the link breakage probability and improves the throughput

Table 12 Throughput for Secure Path Selection Scheme and Link Stability

Node	Throughput for SPSS	Throughput for lspss
40	0.51408 mbps	0.41616mbps
50	0.45696 mbps	0.48144mbps
60	0.41616 mbps	0.61243mbps

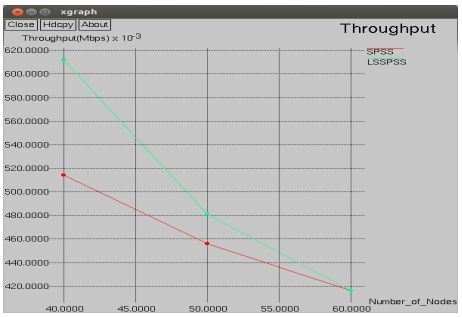


Figure 13 Throughput (X Graph)

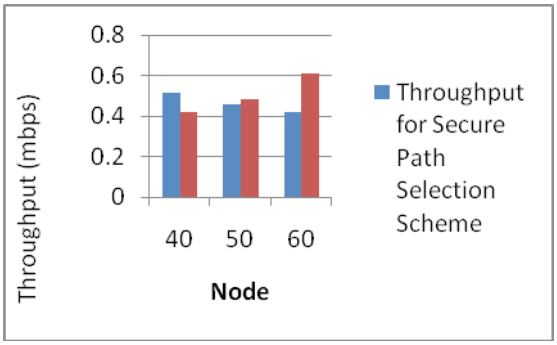


Figure 14 Throughput (Chart)

Conclusion and Future Work

MANET is vulnerable to various security attacks which degrades the security and performance. This research proposed a LSSPSS scheme to improve security and performance of MANET. The SPSS scheme establishes a secure path from source to destination in presence of attackers. It has been successfully injected, detected and also avoided packet dropping node from the active path recovered since trust table established. Some advantages with these mechanisms are: overhead on the network is less. The performance of proposed LS-SPSS is compared against SPSS system using NS2 simulator for varying simulation node. The simulation results show that LS-SPSS improved performance of MANET for packet delivery ratio, throughput and routing overhead.

Future Work

The ad hoc networking is an open challenging area of research in computer science due to its dynamic nature, this means ad hoc network contains lots of vulnerabilities to be explored and many other issues to be solved. In future our plan is to study some other vulnerable areas of mobile ad hoc network. We will also try to configure this proposed mechanism with other mechanism such as other types of security attacks, such as Worm hole attack and Sybil attack.

References

Amol R. Kotkar, Nilesh S.Vani (2016) *"Analysis Routing Protocol in MANET":* April 2006

Babu, M. R., Dian, S. M., Chelladurai, S., & Palaniappan, M. (2015). Proactive alleviation procedure to handle black hole attack and its version. *The Scientific World Journal*, 2015.

Kavitha, P., & Mukesh, R. (2015). To detect malicious nodes in the mobile ad-hoc networks using soft computing technique. In IEEE 2nd International Conference on Electronics and Communication Systems (ICECS), pp. 1564–1573.

Khatawkar, S. D., & Trivedi, N. (2015). Detection of gray hole in MANET through cluster analysis. In 2015 IEEE 2nd International Conference on Computing for Sustainable Global Development (INDIACom), pp. 1752–1757.

Kumar, J. M. S. P. J., Kathirvel, A., Kirubakaran, N., Sivaraman, P., & Subramaniam, M. (2015). A unified approach for detecting and eliminating selfish nodes in MANETs using TBUT. EURASIP

Liu, K., Deng, J., Varshney, P. K., & Balakrishnan, K. (2007). An acknowledgment-based approach for the detection of routing misbehavior in MANETs. IEEE Transactions on Mobile Computing, 6(5), 536–550.

Marchang, N., & Datta, R. (2012). Light-weight trust-based routing protocol for mobile ad hoc networks. IET Information Security, 6(2), 77–83.

Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. In ACM Proceedings of the 6th annual international conference on Mobile computing and networking, pp. 255–265.

Moudni, H., Er-rouidi, M., Mouncif, H., & El Hadadi, B. (2016). Modified AODV routing protocol to improve security and performance against black hole attack. In 2016 IEEE International Conference on Information Technology for Organizations Development (IT4OD), pp. 1–7. Khatawkar, S. D., & Trivedi, N. (2015). Detection of gray hole in MANET through cluster analysis. In 2015 IEEE 2nd International Conference on Computing for Sustainable Global Development (INDIACom), pp.

Shakshuki, E. M., Kang, N., & Sheltami, T. R. (2013). EAACK a secure intrusion-detection system for MANETs. IEEE Transactions on Industrial Electronics, 60(3), 1089–1098.

Sheltami, T., Al-Roubaiey, A., Shakshuki, E., & Mahmoud, A. (2009). Video transmission enhancement in presence of misbehaving nodes in MANETs. Multimedia Systems, 15(5), 273–282.