A Responsive Probing Approach to Detect Dynamic Intrusion in a MANET

Han-Chao Lee[1]
Computer Science and Information Engineering
[1]National Taiwan University of Science and Technology
Taipei, Taiwan
D10315006@mail.ntust.edu.tw

Shin-Ming Cheng[1] , Kuo-Ping Wu[1] and Hahn-Ming Lee[1 2]
[1]National Taiwan University of Science and Technology,
[2]*Institute of Information Science Academia Sinica*
Taipei, Taiwan
{smcheng, wgb, hmlee}@mail.ntust.edu.tw

Abstract—**Mobile Ad hoc NETwork (MANET) is regarded as one of the most appropriate technologies to connect IoT (Internet-of-Things). However, intrusion detection for black hole or flooding attacks in MANET is very complicated due to a lack of trusted centralized authority and dynamic topology. This paper proposes an efficient and effective mechanism, Responsive Probing Mechanism (RPM), to periodically inject probe packets into normal data stream transmission for the dynamic detection of misbehavior intrusion. Moreover, an indicator based on the quality of probe packets transmission is introduced to quantify the degree of misbehavior intrusion. The simulation results show that the proposed RPM outperforms the existing solutions in terms of fast, effective detection and lower calculation cost.**

Keywords—Ad hoc On Demand Distance Vector (AODV); Internet of Things (IoT); Intrusion Detection; Security; Mobile Ad hoc NETwork (MANET).

I. Introduction

With sensing, computation, and communication capabilities, connected nodes can constitute a system to support everyday life in a smart way, which is known as Internet of Things (IoT). Future Internet is embracing the Internet of Things (IoT) concept where smart devices should form fully distributed peripheral networks. The distributed routing paradigm enabled by Mobile Ad hoc NETwork (MANET) fits the requirement of self-managed and autonomic peripheral networks of small objects [1].

Handshaking of MANETs with IoT play significant role in many challenging and advanced application domains like smart cities, traffic management, controlling, monitoring and logistics which definitely encourage the need of development of more secured, challenging and intelligent routing protocols at the intersection of MANETs and IoT [2].

The nodes of IoT have equal status and there is not any central control node in the network. Now a unified standard about IoT routing protocol has not yet appeared. One research shown that routing mechanism of existing routing protocols such as AODV, DRS and OLSR and compare their performance in some given IoT environments. The mechanism of AODV can have better performances in terms of throughput [3]. A research assessed the performance of AODV and DSR in terms of some applications based on Internet of Things (IoT), such as Radio Frequency Identification (RFID) service, voice service and temperature monitoring service. The result shown that DSR has a better performance indoors while AODV can better adapt to outdoor complex electromagnetic environment [4].

However, the AODV routing protocol suffers from various kinds of intrusions or attacks, which should be carefully examined when applying MANET as the network structure of IoT. As a result, threats are quickly evolving to target this new landscape and consequences of IoT security issues are increasingly serious. The first infamous category of attacks is the passive attack, such as eavesdropping, traffic analysis, and location disclosure. The second kind is the active attacks [2], such as the black hole attack, gray hole attack, worm hole attack, sink-hole attack, Denial-of-Service attack, flooding attack and sybil attack. These active attacks receive lots of attentions since they are DOS attack that deprive the traffic from the source node that pose the great threat to the network integrity.

In this paper, we proposed a responsive probing approach to detect various combinations of misbehavior intrusion dynamically happened within a MANET. We proposed a new probing approach, a responsive detection scheme with calculating degree of misbehavior intrusion to identify the existence of dynamic entered misbehaving nodes in routing path based on AODV protocol.

In a practical scenario for IoT in MANET environment, assume there is a group of control nodes deployed in a wide area to continually conduct data stream transmission from source to destination, there is a need exists to dynamically detect and eliminate the misbehaved node's sudden appearance with data packets dropping, decreasing, flooding or delaying.

We use encrypted probe packets to inject into a data transmission path that is not obvious for attackers to discover and circumvent. Also, the probe packets do not affect the quality of data transmission under enough bandwidth in a MANET.

The simulation results show that isolating the misbehavior intrusion nodes can provide a healthy foundation to build a solution for support higher data transfer throughput and quality in a MANET. The probe packets are encrypted so that it is not easy for attackers to discover and of small size so that they do not consume precious bandwidth.

II. Related Work

Intrusion detection in MANET is a lot more complex than in normal wireless networks that are fixed, because it is difficult to collect the required data from the MANET due to dynamic topology and lack of trusted centralized authority [5].

Many types of routing protocols have been developed for MANET. AODV is an efficient protocol which has been widely studied. AODV is a reactive routing protocol that does not require maintenance of routes to destination nodes that are not in active communication. Instead, it allows mobile nodes to quickly obtain routes to new destination nodes [9].

AODV protocol uses three control messages that are Route Request (RREQ), Route Reply (RREP), and Route Error (RERR) [8]. A number of solutions to handle the security issues of AODV have been surveyed and studied [6],[7],[16]~[24].

There are several researches proposed modified AODV routing protocol to detect and prevent the specific black hole attack. Secure AODV (SAODV) [10] mainly incorporates the notion of node authentication at different points during routing of traffic through the network.

Reverse AODV (RAODV) [11] protocol uses a reverse mechanism to create an alternative path in addition to the actual path formed during route discovery phase. RAODV deals with the unavailable link between nodes with lesser routing discovery effort as compared to the AODV protocol thus saving significant computational resources and energy.

PHR-AODV Path Hopping [12] based on Reverse AODV uses multipath communication. It maintains a list of multipath routes available between source and destination nodes. For transmitting the data, paths are selected from this list in sequential order. Broken paths are removed from the list. When the list becomes empty, the source node initiates a fresh routing discovery process to search for new paths.

MAODV [13] solves lost link problem by having such an alternative path prepared beforehand. This routing implementation provides better quality of network services.

Dhaval and Pranav [14] proposed a Permutation based Acknowledgement for most widely used reactive protocol ad-hoc on demand distance vector routing AODV. Recently, K. Kranthi Kumar et al. [15] proposed a leak detection system iterative probing mechanism enables to detect malicious nodes en-route even if they are colluding. A complex control process was presented.

The techniques discussed above are compared in Table I below. Most of the techniques that focus on AODV protocol enhancement and need additional data structure with knowledge support. That would increase the complexity of the system and network processing overhead will increase.

Table I: Comparison of several proposed intrusion detection techniques based on AODV routing protocol in MANETs.

Technique	Advantage	Disadvantage
Secure AODV (SAODV [10])	SAODV mainly incorporates the notion of node authentication at different points during routing of traffic through the network.	(1) All nodes share the same password. (2) An extra computing for authentication is needed. (3) This method is obvious for attackers to discover and take intrusion.
Reverse AODV (RAODV [11])	RAODV protocol uses a reverse mechanism to create an alternative path in addition to the actual path formed during route discovery phase.	(1) The cost of preprocessing the alternative path in addition to the actual path formed during route discovery phase for each node is very high. (2) Extra memory and computing resources are needed.
PHR-AODV Path Hopping [12]	PHR-AODV Sending data through different routes minimizes the severity of attacks by malicious nodes considerably.	The cost of preprocessing the different routes for each node is very high and extra memory and computing resources are needed.
MAODV [13]	MAODV Solves lost link problem by having such an alternative path prepared beforehand that provides better quality of network services.	The cost of maintaining the alternative path for each node is very high and extra memory and computing resources are needed.
Adaptive Acknowledgement (AACK [14])	An enhancement of Adaptive Acknowledgement (AACK) and TWO-ACK of AODV. A Permutation based Acknowledgement proposed for most widely used reactive protocol AODV.	(1) Incrementing number of messages routed in the network. (2) Extra memory and computing resources are needed.
Leak Detector System Iterative probing Mechanism [15]	Iterative probing mechanism enables to detect malicious nodes en-route even if they are colluding.	(1) It needs to apply complex probing process and share lots of information between each legitimated nodes. (2) It is not easy for a leak detection mechanism to find the values in data packets has been tampered.

III. PROPOSED RESPONSIVE PROBING MECHANISM (RPM)

We proposed a Responsive Probing Mechanism (RPM). Encrypted probe packets are periodically forward from the selected source node to the destination node by injecting into the regular data transmission path. A responsive probing strategy applied to autonomously reduce the scope of new probing path based on the quality of arrived probe packets.

A. Scenario

In a MANET, assume there is a group of control nodes $N_{i(i=1\sim5)}$ deployed in a wide area as shown in Fig. 1. for transmitting data stream continuously from the source (N_1) to the destination (N_5) at time T_0. There are two malicious nodes X_1 (at the time T_a) and X_2 (at the time T_b) dynamically entered into MANET for the purpose of fixing routing path or maybe carried with the misbehavior intrusion of dropping, decreasing, flooding or delaying packets.

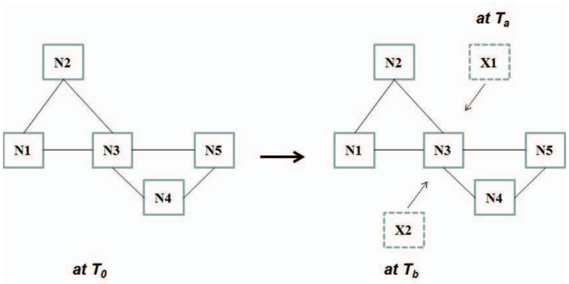

Fig. 1: A scenario of dynamically entered nodes in a MANET.

In this paper, we proposed a responsive intrusion detection scheme with probe packets injected in normal data transmission to discover the misbehaving nodes that caused data transferred with dropping, modifying or delaying packets in a given prearranged routing path from the source node to the destination node as shown in Fig. 2. (a).

We have considered three basic types of intrusive behavior, combined with probing packets dropped, modified, and delayed, shown in Fig. 2. (b)(c)(d) associated with the different degree of misbehavior intrusion in a MANET.

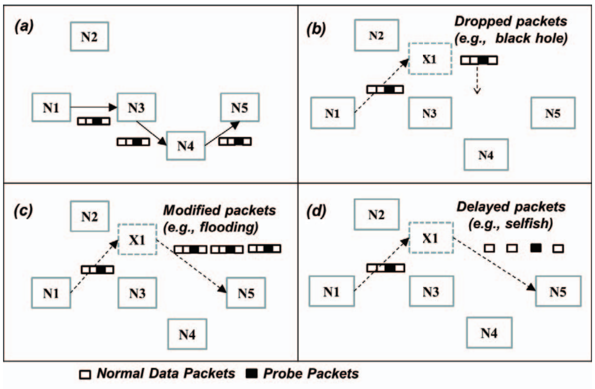

Fig. 2: The scenarios of RPM in a MANET with various misbehavior intrusions.

B. Equations

In our proposed RPM intrusion detection scheme, we defined notations as follows to describe the set of control nodes and dynamically entered nodes in a MANET environment.

T_i : a time period for each probing process.

$L_{T_i} = \{N_j \mid 0 \le j \le n\}$: a set of trusted legitimate nodes in T_i .

$M_{T_i} = \{X_j \mid 0 \le j \le m\}$: a set of unknown new entered nodes in T_i (X_j maybe a legitimate node or a malicious node).

$O_{T_i} = L_{T_i} \cup M_{T_i}$: a union set of nodes in a MANET in time period T_i

We calculate the Degree of Misbehavior Intrusion (DMI) *(1)* from the selected destination node which provides an indicator to identify the degree of malicious nodes existence from the source node. A responsive probing strategy autonomously applied to reduce the new probing path scope based on the data transfer quality by DMI indicator calculated from the probing packets received. The definition of DMI equation and parameters derived from arrived probe packets are shown as follows:

$$q_1 = \frac{\text{number of Probe Packets dropped}}{\text{total number of Probe Packets}} \times 100\% \qquad (1)$$

$$q_2 = \frac{\text{number of Probe Packets modified}}{\text{total number of Probe Packets}} \times 100\% \qquad (2)$$

$$q_3 = \frac{\text{time delay to deliver Probe Packets}}{\text{expected time taken to deliver Probe Packets}} \times 100\% \qquad (3)$$

$$DMI(N_s, N_d, T_i) = \sum_{i=1}^{3} w_i q_i, 0 <= w_i <= 1 \qquad (4)$$

(1),(2),(3) represents the Probe Packets Deliver Ratio, Probe Packets Modified Ratio, and Probe Packets Delay Ratio derived from probing packets received from the source node $N_s \in O_{T_i}$ to the destination node $N_d \in O_{T_i}$.

the DMI indicator (4), represents the misbehaving intrusion degree from the source node N_s to the destination node N_d at T_i .The w_i is a weight parameter, representing the degree of influence for each type of intrusive behavior.

$S = \{(N_s, N_d, T_i) \mid DMI(N_s, N_d, T_i) > z, z >= 0\}$, represent a set of suspicious routing path from N_s to N_d with the value of DMI is greater than threshold z (z is a configurable value for sensitivity of misbehaving intrusion).

C. Detection Scheme

The RPM intrusion detection scheme is designed for intrusion detection by iteratively injecting encoded packets into the routing path. We illustrated data packets flow in a series of probing process iteration shown in Fig. 3. At time T_0 , a scheduled encoded packets from source node N_1 to destination node N_5 . At time T_0 , $DMI(N_0,N_5,T_0)$ is calculated from probing scope from source node N_1 to the destination node N_5 , and zero value of DMI represents there is no misbehaving nodes from N_1 to N_5 .

At time T_1 , in the next scheduled probe packets period, X_1 acted as a misbehaving node dynamically entered in the routing path area between N_2 and N_3 which caused N_3 didn't received any scheduled encoded packets from N_2 or maybe got less or much more packets than expected in other condition.

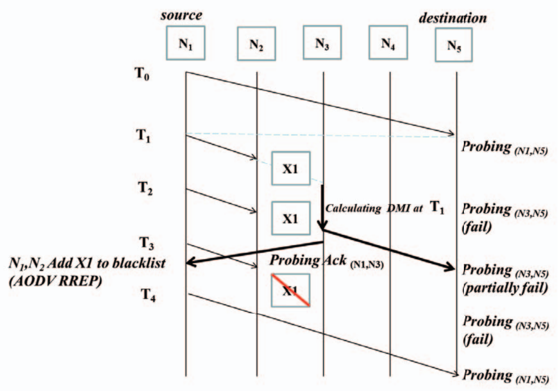

Fig. 3: An example of RPM probing process iteration.

At time T_1 , in the next scheduled probe packets period, X_1 acted as a misbehaving node dynamically entered in the routing path area between N_2 and N_3 which caused N_3 didn't received any scheduled encoded packets from N_2 or maybe got less or much more packets than expected in other condition.

When time out occurred in this special show case, N_3 behaved automatically as the new source node to send encoded probing packets to destination node N_5 , the value of $DMI(N_1,N_3,T_1)$ is calculated and greater than zero which represents there are misbehaved nodes found from N_1 to N_3 . N_3 will issue AODV RREP packets to broadcast the malicious nodes X_1 found for N_1 and N_2 to add $S\left(N_{2,3},T_1\right)$ into its blacklist for eliminating misbehaved nodes.

D. System Architecture

The solution that we propose here is designed to detect and find the dynamically joined misbehaving nodes. The probing intrusion detection system architecture is shown in Fig. 4. A probing timer inside a control node is used to periodically inject probing packets into the normal data packets sent.

When a node acts as a neighborhood to forwarding data packets received or time out event occurs, it automatically calculates the DMI value to detect misbehaving nodes happened and broadcast data link error and malicious nodes found by sending AODV RERR and AODV RREP packets through wireless sensor channel.

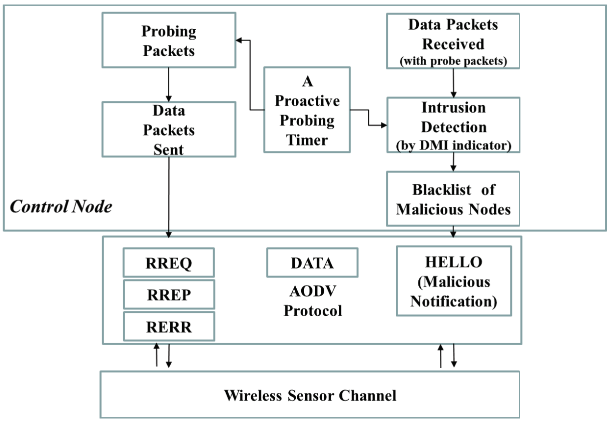

Fig. 4: System architecture of RPM.

When a node acts as a neighborhood to forwarding data packets received or time out event occurs, it automatically calculates the DMI value to detect misbehaving nodes happened and broadcast data link error and malicious nodes found by sending AODV RERR and AODV RREP packets through wireless sensor channel.

A probing packet flow diagram is shown in Fig. 5. The probing process starts from an initialized probing path at pre-scheduled time period to continuously forwarding probing packets from the source node to the destination node, and responsively choosing the re-probe path scope in the next iteration that with the most likely chance to identify the existence of misbehaving nodes.

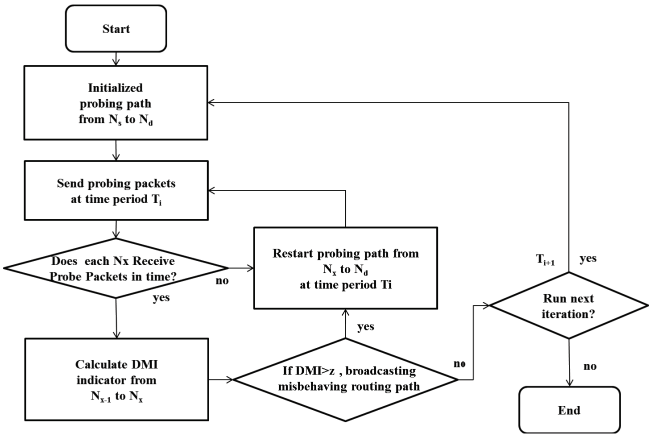
Start
Initialized probing path from N_s to N_d
Send probing packets at time period T_i
Does each Nx Receive Probe Packets in time?
no
yes
Restart probing path from N_x to N_d at time period Ti
Calculate DMI indicator from N_{x-1} to N_x
If DMI>z , broadcasting misbehaving routing path
yes
no
Run next iteration?
T_{i+1}
yes
no
End

Fig. 5: A probing packet flow diagram of RPM.

If probing process encountered time out event or DMI value is exceed zero in some node, a new probing packet flow will restart from the node. Any suspicious path found will be broadcasted by AODV acknowledge back to all control nodes for elimination of all new entered nodes collected in the suspicious routing paths found.

IV. SIMULATION

To find the effect of our proposed approach and system to detect the misbehaving attacker in a MANET system, we do some experiments as below.

The main objective of simulation is to prove the proposed RPM is properly securing the existing AODV away from dynamically joined malicious nodes attacking.

One black hole node is dynamically created, the result of simulation with the Network Simulator Version-2 (NS2) simulation parameters listed in Table II. Performance matrix of our simulation is probing packets delivery ratio.

Table II: Simulation parameters

Simulator	NS-2 (ver.2.35)
Simulation time	50 sec.
Number of mobile nodes	50
Number of malicious node	1~3
Topology	600m × 600m
Transmission Range	200m
Routing Protocol	AODV
Maximum Bandwidth	0.1Mbps
Traffic	Constant bit rate
Packet Size	1600

For simulation, we have considered three phases i.e., initial phase without malicious nodes, and second phase with new entered nodes with misbehavior (as shown in Fig. 6, Fig. 7). In below tabs show our considered network scenarios.

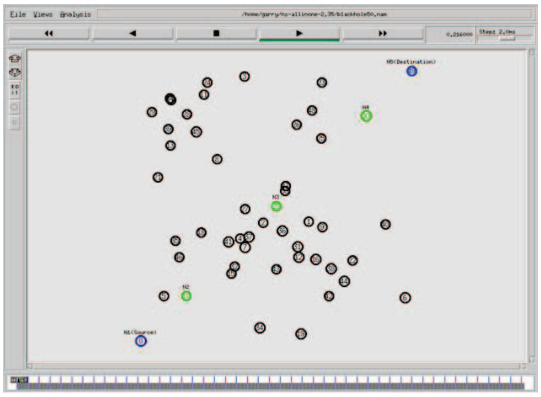

Fig. 6: Initial phase without any malicious node.

Due to dynamic nature of the MANET, its network becomes open to attackers and unreliable. The node misbehavior such as a black hole attack could significantly downgrade the performance (there is no packets reach the destination), so in our simulation we are going to calculate Degree of Misbehavior Intrusion (DMI)[a.] under the condition of misbehaving nodes existence.

[a.] (Parameters: $w_1 = 0.5, w_2 = 0.3, w_3 = 0.2$, and $z = 0$)

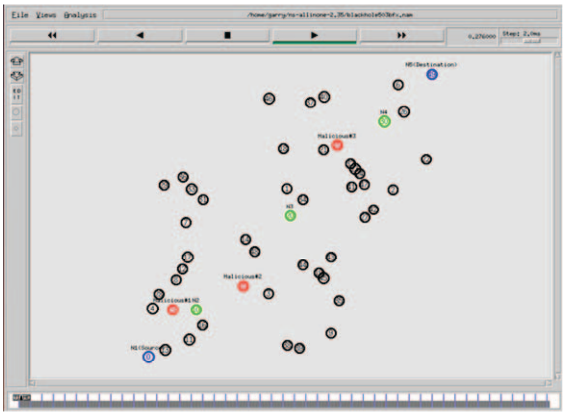

Fig. 7: The second phase with new entered malicious nodes. (labelled with malicious node # tag)

[b.] Packet Delivery Ratio (PDR) is the ratio of data packets delivered to the destination to those generated by the constant bit rate sources. As the calculation, Packet Delivery Ratio = No. of Packets Received / No. of Packets Sent * 100.

Packet Delivery Ratio[b.] is an important metric to show how successful a proposed protocol performs delivery packets from the source node to the destination node. Fig. 8. Represents the different PDR performance from 50 randomly generated nodes contains zero, one, two and three malicious nodes with RPM vs without RPM in the simulation time period. It showed out that RPM do get rid of malicious node attacks and keep repairing data transmission path to support higher data transfer quality in a MANET. The packet delivery ratio is sustained even with the existence of malicious nodes in the network when the proposed probing mechanism is applied.

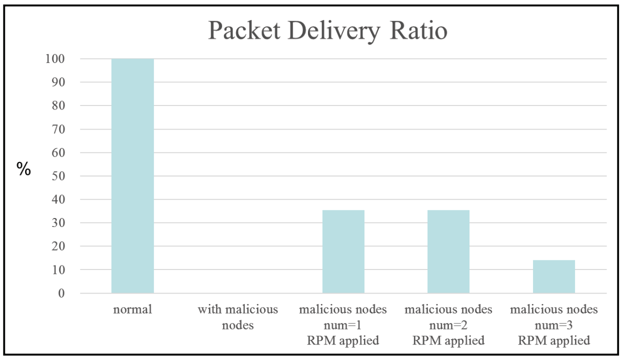

Fig. 8: Comparison of Packet Delivery Ratio.

V. CONCLUSION AND FUTURE WORK

The detection of malicious node mechanism for MANET and AODV routing protocol has the most significant work has been done and proposed in this area. We have proposed a more general attack detection mechanism to identify the existence of dynamically entered misbehaving nodes efficiently, to increase overall throughput.

In this paper, we have proposed an efficient and effective routing method with a probing technique with a Degree of Misbehavior Intrusion (DMI) indicator and a quick, responsive detection scheme to identify the existence of dynamic jointed misbehaving nodes at its nearby area in a MANET based on AODV routing protocol. It does not require any database and significantly more processing power.

In Future, we will find out a more adaptive detection scheme by parameters (w_i ,z) learning and put our best efforts to making out more efficient probing technique with minimized messages overhead to detect dynamic intrusion in MANETs.

ACKNOWLEDGMENT

This work is supported in part by the Ministry of Science and Technology of Taiwan under grants number MOST 102-2218-E-011-011-MY3, 104-2221-E-011-051 and 104-2923-E-011-006-MY2.

REFERENCES

[1] A. R. Tipu, O. Adigun, A. Ladas, N. Weerasinghe, “Towards a Scalable Routing Approach for Mobile Ad-hoc Networks,” Computer Aided Modelling and Design of Communication Links and Networks (CAMAD), 2015.

[2] M. Rath, U.P. Rout, “Analysis and Study of Security Aspect and Application Related Issues at the Junction of MANET and IoT,” International Journal of Research in Engineering and Technology (IJRET), Vol. 4 Special Issue 13, 2015.

[3] H.M. Xin, K. Yang, “Routing Protocols Analysis for Internet of Things,” International Conference on Information Science and Control Engineering (ICISCE), 2015.

[4] S.F. Hou, M.Q. Wu, , W.X. Liao, D.Y. Wang, “Performance Comparison of AODV and DSR in MANET Test-bed Based on Internet of Things,” Vehicular Technology Conference (VTC Fall), 2015.

[5] P. Peethambaran, J. S. Jayasudha, “Survey of MANET Misbehaviour Detection Approaches”, International Journal of Network Security & Its Applications (IJNSA), Vol. 6, No. 3, 2014.

[6] P. Rajakumar, V. T. Prasanna, A. Pitchaikkannu, “Security attacks and detection schemes in MANET,” Electronics and Communication Systems (ICECS), 2014.

[7] A. Saeed, A. Raza , H. Abbas, “A Survey on Network layer Attacks and AODV Defense in Mobile Ad hoc Network”, IEEE Eighth International Conference on Software Security and Reliability-Companion (SERE-C), 2014.

[8] K. Patel , P. Patel, “Simulation and Performance Evaluation of AODV protocol against Blackhole Attacks in MANET,” International Journal of Engineering and Technical Research (IJETR), Vol. 2, Issue 5, 2014.

[9] D. Gupta, R. K. Gujral, “Simulation of Different Routing Protocols in MANET Using NS2,” International Journal of Scientific and Research Publications, Vol. 4, Issue 8, 2014.

[10] S. Deswal, S. Singh, “Implementation or Routing Security Aspects in AODV,” International Journal of Theory and Engineering, Vol. 2,Issue 1, 2010.

[11] P. Bathla, H. Gupta, “Security Enhancements in AODV Routiing Protocol,” International Journal of Computer Science and Technology, Vol. 2, Issue 2, 2011.

[12] E. Talipov, D. J. Jin, I. H. Junghoi, Y. Choi, C. Kim, “Path Hopping Based on Reverse AODV for Security,” Springer, APNOMS, 2006.

[13] M. Sefrati, A. Bilami, M. Benmohamed, “MAODV, AODV Variant to Improve Quality of Service in MANETs,” Inernational Journal of Computer Science Issues, Vol. 8, Issue 1, 2011.

[14] D. Dave, P. Dave, “An Effective Black Hole Attack Detection Mechanism using Permutation Based Acknowledgement in MANET,” Advances in Computing, Communications and Informatics (ICACCI), 2014.

[15] K. K. Kranthi, L. CH. Vasantha, K. Srinivasa Rao, “Identifying the behavior: Nodes, Route and Collusion Attack's in MANET,” International Conference on Contemporary Computing and Informatics (IC3I), 2014.

[16] K. Chadha, S. Jain, “Impact Of Black Hole And Gray Hole Attack In AODV Protocol,” International Journal of Scientific and Research Publications, Vol. 4, Issue 8, 2014.

[17] A. Siddiqua, K. Sridevi, A. Ahmad, K. Mohammed, “Preventing Black Hole Attacks in MANETs Using Secure Knowledge Algorithm,” International Conference on Signal Processing And Communication Engineering Systems (SPACES), 2015.

[18] T. Varshney, T. Sharmaa, P. Sharma, “Implementation of Watchdog Protocol with AODV in Mobile Ad Hoc Network,” Fourth International Conference on Communication Systems and Network Technologies, 2014.

[19] G. S. Baghel, V. Chourewar, “An Efficient Malicious Nodes Detection in MANETs using OPNET,” International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, Issue 8, 2014.

[20] T. Manikandan, S. Shitharth, C. Senthilkumar, C. Sebastinalbina, N. Kamaraj, “Removal of Selective Black Hole Attack in MANET by AODV Protocol,” International Conference on Innovations in Engineering and Technology (ICIET’14), Vol. 3, Special Issue 3, 2014.

[21] S. Balamurugan, V. Kanmani, S. Radhika, “Black Hole Detection in AODV Using Hexagonal Encryption in Manet’s,” International Journal of Modern Engineering Research (IJMER), Vol. 4 , Issue. 12, 2014.

[22] S. K. Dhurandher, I. Woungang, R. Mathur, P. Khurana, “GAODV: A Modified AODV Against Single and Collaborative Black Hole Attacks in MANETs,” 27th International Conference on Advanced Information Networking and Applications Workshops, 2013.

[23] J. K. Mandal, K. L. Hassan, “A Novel Technique to Detect Intrusion in MANET,” International Journal of Network Security & Its Applications (IJNSA), Vol. 5, No. 5, 2013.

[24] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, Y. Nemoto, “Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method,” International Journal of Network Security, Vol. 5, No. 3, 2007.