American Journal of Applied Sciences

Original Research Paper

Performance Evaluation of Blackhole Attack on AODV in VANET

Taha Saad

Computer Science and Information Technology, University Putra Malaysia, Malaysia

Article history
Received: 12-02-2017
Revised: 07-09-2017
Accepted: 31-10-2017

Email: tahasaadcsit@gmail

Abstract: Black hole is one of the ongoing network threats that impact the physical components of Vehicular Ad hoc Networks (VANETs) when more layers deal with routing mechanism of vehicular ad hoc network. An algorithm for Ad hoc On-Demand Distance Vector (AODV) protocol in VANET was developed in order to identify collaborative group of nodes that behave as black hole. The simulation was configured to perform three scenarios with number of nodes set to 10, 20 and 40 nodes respectively. The result showed that the proposed algorithm provides a better throughput performance, less end to end delay, high packet delivery ration, less packet drops and less time for processing the incoming and outgoing nodes. Future works may consider testing the proposed solution on other types of attacks such as Wormhole, Jellyfish and Sybil attacks.

Keywords: VANETs, Balckhole Attack, AODV

Introduction

The current efforts devoted to prevent black hole attacks in VANETs have been claimed to be a challenging task (Medina *et al*., 2016) in which Ad hoc network can be found orderly, centralized and open milieus. In with any of these milieus, the security is the issue that it should be considered with the highest priority. Nodes in each of these milieus are mostly menaced via the same safety problems. However, there are some safety issues which are particular to that medium than the others requirement (Sharma *et al*., 2015). Large numbers of unstructured nodes and the obscurity of a priori relations are several of the major features of unlock medium ad hoc networks. These networks are fully comparable to the centralized medium networks, but the greater quantity of nodes lead the nodes in the unlock medium to be exposed to more sophisticated safety attacks than the centralized networks work (Choure and Sharma, 2013). For example, nodes in both unlock and centralized milieus know from the obscurity of a centric authority. Security could as well be readily performed in the orderly medium because nodes in which medium are commonly equipped with suitable safety tools before taking part into any particular tasks such as in a martial operation (Nafaa and Ghanemi, 2014).

In the context of VANET, vehicles are typically armed with a series of processors and sensors in the near future. The sensor is responsible of capturing the real physical data related to the car engine and performance. Then, uses the processed data to supply the main car processor as well as the driver. Moreover, it is assumed that vehicles as a result can secure data from another vehicle in their proximity and from RSUs. In the perspective of safety requirements, integrity of the messages have to be warranted, albeit preserving at the same time the user's particularity. Another application, e.g., multimedia import allocation, may also want to encrypt their passing to avert eavesdropping from non-registered users. The utilize of Certification Authorities (CAs) and general key cryptography to conserve Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) connection achieves most safety requirements (Tyagi and Dembla, 2014).

Attackers might select to start their attacks versus the net individually or collectively. Elementary attackers commonly create a temperate transit carry as long as they are not eligible to arrive any cable facilities. As it becomes much costly for the elementary nodes to separate the encrypted messages, nodes in the nets could ration the costly cryptography task with every another by working collaboratively various connections they had amongst them (Ahmed *et al*., 2014). However, if some attackers are organizing to initiate attacks, defending the ad hoc nets will be a complex task. This is because collaborative attackers could readily close any elementary node in the net and be competent to degrade the capacity of network's divided procedures including the safety techniques. Hence, we addressed the current problem of collaborative black hole attack for AODV protocol in VANET. This is mainly because of that most standard protocols utilized with VANET are not capable to treat the mentioned security issues (Nadeem and

Science Publications

Howarth, 2013). In addition, attacker nodes are usually use ancient datum, amend routing datum and increase the load on the network leading to block suitable routing protocol functioning. As such, collaborative malicious nodes will be more sophisticated in coordinating the attack against a MANET or in our case a particular VANET. Thus, we proposed the development of an algorithm for AODV protocol in VANET in order to identify collaborative group of nodes that behave as black hole.

Vanet Related Attacks

VANETs have been addressed to experience various threats and attacks due to the misconfiguration of one component with another (Kasiran and Hassan, 2013). This is also reasoned to that most vehicle provide the required source of electricity in which some components such as OBU is not responsible for tolerating the bottleneck of limited battery life as compared to other components in network (Pathan, 2016). Hence, the integrity of OBU with other components can provide the necessary network antecedents to grant access to the vehicle computing capability in normal ad-hoc networks. As such, identifying the different types of attacks in VANET can help us to understand the unique nature of vulnerabilities and various kinds of attacks (Dixit *et al*., 2015).

The literature showed that the potential VANET threats and attacks on several network components in terms of confidentiality, integrity, authentication and identification and availability are typically occurred based on the cryptographic categorization of standard network security. Other attacks in terms of authentication and accountability. With this regard, availability of a network is the main focus of this study in which black hole attack is being studied.

Blackhole

Security is one of the ongoing issues in VANET environments in which various studies were conducted to overcome its consequences on networks' overall performance. Black hole is one of these threats whereas the physical components of VANET are experiencing potential threats when more layers deals with routing mechanism of vehicular ad hoc network (Kaushik and Tayal, 2016). Previously, the nature of attack on a network has been always looked at from the purpose of not processing and sending feedback through routing mechanism (Lee and Jeong, 2016). This has been addressed to impact the way of how sequence number and hop count in a network. In light of this, malicious vehicle of Black hole attack does not usually spear time to process the neighbors' nodes in order to initiate a Route Request packet (RREQ). For example, when a packet transmitted from the source to the destination, the RREP will monitor the packet's state by sending a false pack*et al*ong with another sequence number when a request reaches the vehicle (Baiad *et al*., 2016). This help to keep the network informed about the status of a packet when traveling from the source to the destination. A malicious vehicle here may occur when submerge of all data packets is not distributed according to the nodes. As such, it is assumed that securing nodes in a network under AODV protocol is vulnerable to such type of attacks (Sharma *et al*., 2015). This can be reasoned to that network centric property is usually placed within the AODV in which vehicle covered by a network must shares their routing tables among each other. With this in mind, some modification of the shared information in a network may results in false stream that can be acted as clear sign of Black hole attack.

On the other hand, AODV can be viewed as a vulnerable protocol to Black hole attack because it relays on the number of sequence to indicate the status of information transmitted through network routes. In addition, in the event of having multiple routes, RREQ identify the sequence number with highest value whereas it is used later to compare with other sequence number of multiple routes (Kumar and Bhardwaj, 2015). If the sequence number matches, then the vehicle select the route that consists of less number of hops. Then, a malicious vehicle sends Route Reply (RREP) messages without checking its routing table where the source vehicle 0 shown above generates a RREQ message to discover a route for sending packets to destination vehicle 2. A RREQ broadcast from vehicle 0 is received by neighboring vehicles 1, 3 and 4 (Bibhu *et al*., 2012). This led many researchers to propose the need for increasing the level of trust of a message when transferring between different hops.

Previous Studies

A number of studies have been proposed in the literature to provide a better solution for detecting and examining different network related attacks. The literature showed the needs for studies to enhance the current detection of a network when experiencing Black hole attack. For example, Djenouri *et al*. (2009) proposed a solution to detect and isolate Black hole in MANETs. The technique involves casual two-hop ACK is used. Results showed that the tow-hop ACK has significantly reduced the cost with lower artificial revelation than normal two-hop ACK sketch. They presented an optimization solution using Bayesian technique for detecting Black hole attacks. The proposed method featured no periodical packets exchanging leading to overhead elimination. Jotangiya *et al.* (2016) proposed a new method for AODV protocol to examine and prevent potential Black hole attack using the trust mechanism. This mechanism was used to help finding the malicious node and then prevents that node in order to ensure a better communication of nodes and gives the exact data sent from source node to destination node. The result showed that the proposed method offered greater loss of data and degradation in performance of the network. As such, it can be concluded that AODV can be further secured by providing a more comprehensive method for ensuring node's security. Arya *et al.* (2015) presented a Trusted AODV routine protocol. The procedure involved that nodes implement trusted routing conduct according to the trust relationship amongst among them. The routing protocol is embedded in the trust mission itself. The connection amongst these nodes relied on the trust level among these nodes. However different threshold functions are utilized to define the reliability or unreliability of the neighborhood nodes. Alheeti *et al.* (2015) worked on detection system for malicious nodes in VANET. The work developed a real-time revelation and isolation of the malignant vehicles. The detection depends on the features removed from the effect file which were created using network simulation. The remark in this work is that the information that was used to build the intrusion detection system was taken from the simulation itself based on one scenario that is Manhattan Urban Mobility only rather multiple scenarios.

Method

This study considered enhancing the detection of black hole for AODV protocol in VANET. NS2 was used in this study to simulate the proposed algorithm based on certain parametrical values.

Proposed Algorithm

The main process starts with examining the available node in a network, which involves checking whether RREQ receive the packet first, if it is, then a confirmation message will be sent back to the RREP packet. This was essential to indicate any potential gap in node destination. In the event that the compared destination is not the same, then it checks its routing table to determine if it has got a route to the required destination. If not, it replies the RREQ packet by distributing the node destination details with other neighbors. If its routing table contains an entry to the destination, then the next step is comparing the destination sequence number in its routing table to that present in the RREQ packet. The following sequence explain the proposed steps in terms of send, reply, receive and conditional:

```
1)      S sends RREQ;
2)      RREPN replies with RREP;
 if RREPN not a Black hole then
 RREPN Sends CONFIRM Packet to D
 via the route
 for D;
 end
3)      S receives RREP;
 if RREPN in Black hole Table then
 Discard RREP;
end
else if RREP from IN then
Send CHCKCNFRM packet to D via route
advertised by RREPN;
end
else
route data;
end
4)      if IN receives CHCKCNFRM and
        had received
  CONFIRM then
  IN unicasts (on the same route as
  CHCKCNFRM)
  REPLYCONFIRM to the source;
  End
5)      if S receives REPLYCONFIRM from
        IN then
  checks in its checktable and updates
  checktable and
  Stores appropriate relay values;
  End
6)      if S receives REPLYCONFIRM from
        D and S doesnt
  time out then
  Deletes check table;
  Routes the data;
  end
  else
  process checktable;
  stores in collaborative Black hole list the
  IDs of nodes starting From RREPN uptil
  all the nodes
  until relay value 0 reached;
  Retry RREQ;
  End
```

When one node receives the CONFIRM packet, the node set the "isRecvConfirm" flag with TRUE. If one node receives the CHCKCNFRm packet, the node sends the REPLYCONFIRM packet. If source node receives the REPLYCONFIRM packet from the IN, it updates the check Table and set the relay value in the "receive REPLYCONFIRM" function.

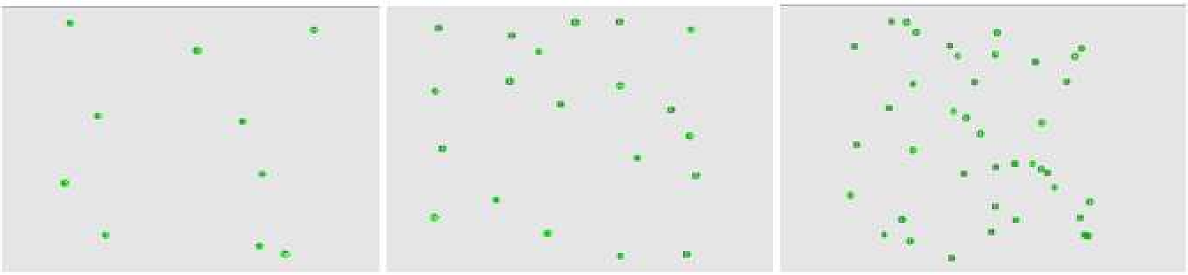
If source node receives the REPLYCONFIRM packet from the destination, it deletes the check Table and set the OK flag with TRUE. If the OK flag is set with TRUE, then the data will be sent via routing protocol. If the source does not receive the REPLYCONFIRM packet without time out, the detection about black hole is run by the "DetectCollaborativeBKs" function.

Simulation Setup & Topology

The developed algorithm is based on a modified AODV protocol, initially, introduced by (Ahmed *et al.*, 2014). The simulation parameters that were selected in this study is illustrated in Table 1.

Table 1: Planned simulation parameters

Examined protocol	AODV
Simulation time	500 sec
Simulation area (m × m)	1000 ×1000
Number of nodes	10, 20 and 40
Number of attacks	0, 2 and 6
Performance parameter	Throughput, end-to-end delay, PDR and packet dropped
Pause time	100 sec
Mobility (m/s)	10 m/sec
Packet inter-arrival time (s)	exponential (1)
Packet size (bits)	exponential (1024)
Transmit power(W)	0.005
Date rate (Mbps)	11 Mbps
Mobility model	Random waypoint



A: 10 nodes B: 20 nodes C: 30 nodes

Fig. 1: Simulation scenarios with 10 nodes

VANET topology was used in this study based on three scenarios. The first scenario consists of 10 nodes; second scenario consist of 20 nodes; and third scenario consists of 40 nodes as shown in Fig. 1.

Performance Metrics

Since this study aim at improving the performance of a network, then a number of performance metrics were considered. For example, we examined the performance of the proposed algorithm in NS2 based on the throughput, end to end delay, packet delivery ration and time. The result obtained from these metrics were also compared to the work of Ahmed *et al*. (2014).

1) Throughput

$$\text{ThroughPut} = \frac{\text{Received DataSize Bits}}{ReceivedTime - SentTime}$$

2) End to End Delay Time

$$\text{DelayTime} = \text{PacketReceivedTime} - \text{PacketSentTime}$$

3) Packet Delivery Ratio

$$\text{PDR} = \frac{\begin{array}{c} Number\ of\ Sent\ Packet \\ -Number\ of\ Received\ Packet \end{array}}{Number\ of\ SentPacket} \times 100$$

4) Packet Dropped

$$\text{Packet Dropped} = \text{Number of Sent Packet} - \text{Number of Received Packet}$$

5) Time

$$\text{Time} = \text{Time}_{Energy\ of\ all\ Nodes\ equals\ 0} - StartTime$$

Results

The examination of performance was based on monitoring network performance when inducing six black hole attacks. The performance results from using the proposed algorithm in these three scenarios were compared to the previous work of Ahmed *et al*. (2014) in order to provide the necessary insights about the feasibility of the proposed solution.

The obtained results mostly showed that the proposed algorithm was found to outperform the algorithm in previous work. For example, Fig. 2 shows the throughput results for both algorithms when experiencing six black hole attacks. From the result, it can be concluded that our algorithm provided a comprehensive throughput performance which increases whenever the number of nodes increase. In addition, we also noted that although the operations of black hole attacks and neighbor attacks are different, the degree of damage to the throughput performance was minimal when comparing it to the throughput of previous work.

As for the end to end delay performance, the comparison results shown in Fig. 3 revealed that the proposed algorithm provided a reliable performance in the first and second scenarios. However, a noticeable drop in delay can be noticed in the third scenario. This can be reasoned to that the proposed algorithm attempts to accomplish route discovery process when experiencing multiple black hole attacks in which the replay from black hole with a false route to the destination may cause additional delay. This is mostly apparent in the case of having high number of nodes with multiple black hole attacks.

The packet delivery ration is shown in Fig. 4 revealed that the proposed algorithm provided better packet deliver ration in all the scenarios as compared to the algorithm in previous work. The proposed algorithm seems to effectively monitor nodes' state when more attackers are present. For example, the more delivery ration can be contributed to the packet traveling time in which more packets were able to reach destinations.

Figure 5 shows the packet dropped number in both algorithms for six black hole attacks. It can be said that the proposed algorithm still offers a significant improvement in packet dropping rate even when the black hole attacks are increased. This can be reasoned to that the proposed algorithm was able to accelerate the sending process of target node to the sender when a packet drops ratio increases. On the other hand, the reason why the algorithm in previous work was not offering the desirable results can be due to that unauthorized route request would fail verification and be dropped by each of the requesting node.

Figure 6 shows the time requires for an algorithm to successfully process node's information when experiencing six black hole attacks. The overall result showed that our algorithm provided the necessary antecedents that facilitate the process to identify node's state when checking for the number of dropped packets. In the previous work, the time required to transfer nodes is longer due to that node may drop packets due to broken links.

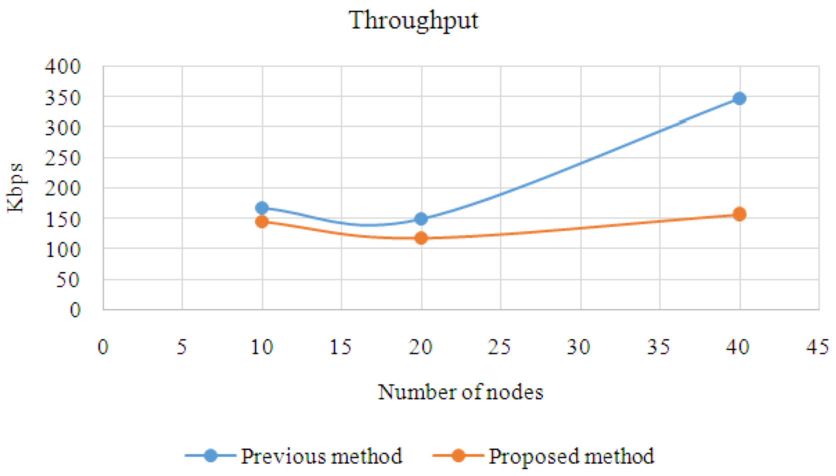


Fig. 2: Throughput results for six black hole attacks

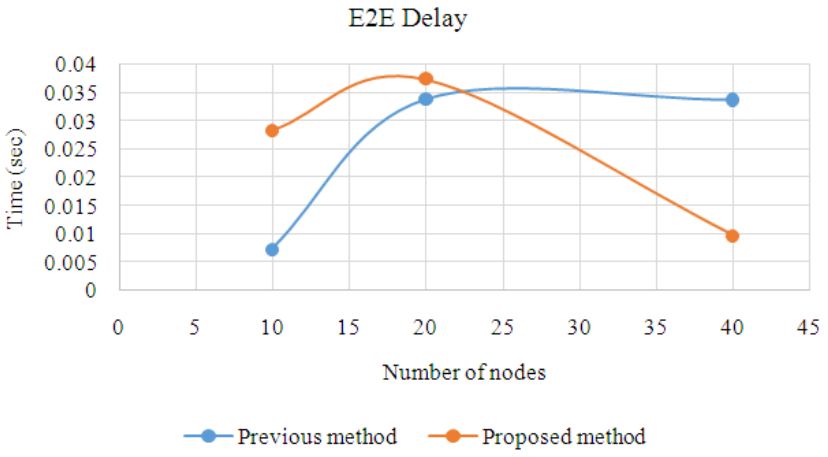


Fig. 3: End to end delay results for six black hole attacks

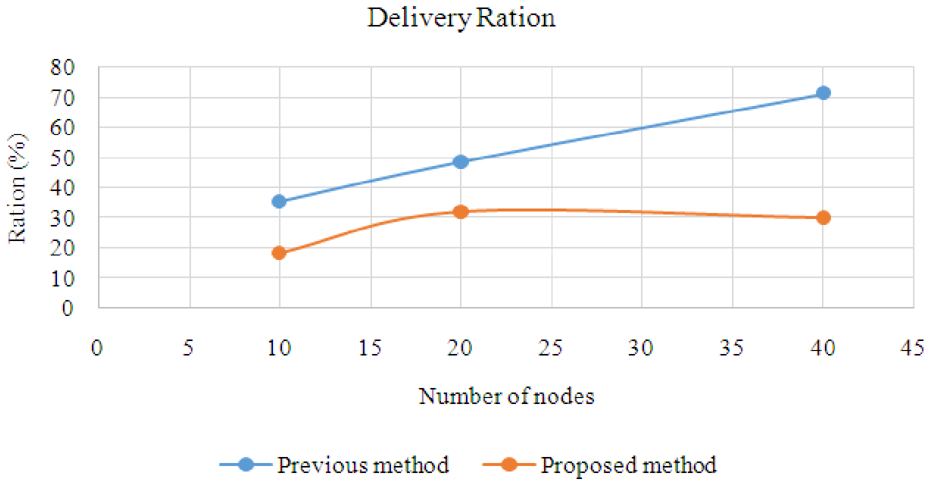


Fig. 4: Packet delivery ration results for six black hole attacks

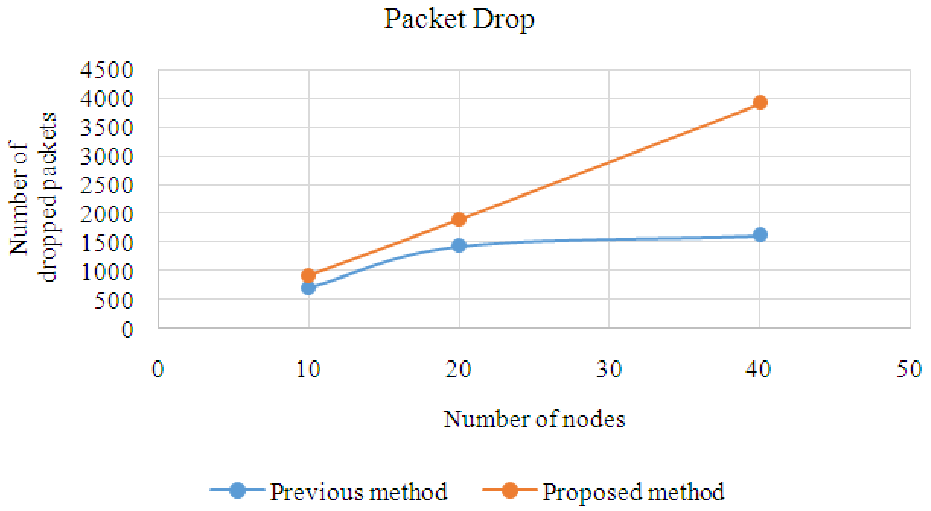


Fig. 5: Packet dropped results for six black hole attacks

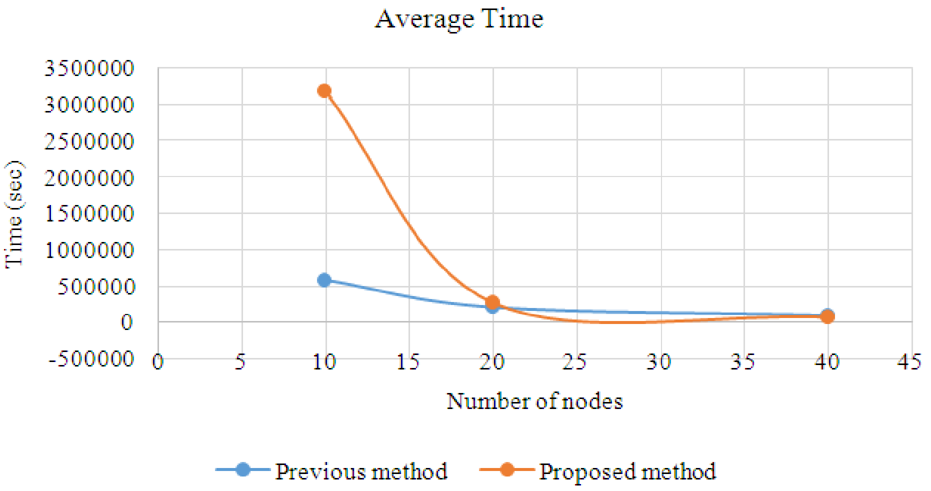


Fig. 6: Time results for six black hole attacks

Discussion

This study found that the proposed solution increased the throughout value of a network when increasing the number of black hole dramatically. Such aspect has been characterized by Kaur and Bansal (2015) as the lack of proper method for examining and predicting black hole in multiple node attacks. For example, Bibhu *et al.* (2012) stated that when disabling the reply messages in VANET, the performance result can be improved based on the delivery of message. This is also believed to secure the network from Black hole attack as it is the case in the present study. On the other hand, the proposed method was also found to reduce the end-to-end delay rate when comparing it with another previous work. Based on the survey conducted by Al-Kahtani (2012; Zeadally *et al.*, 2012), delay in a network can be caused due to the lack in authenticate and validate transmitted message in the network. Hence, the proposed solution can be said to provide a reliable authentication of the transmitted messages within multiple nodes in VANET. Varshney *et al.* (2014) addressed that black hole attach usually attempt to send route response incorrectly to destination with minimum hop count which results in slowing down the packet delivery ration based on this malicious node in a network. However, the proposed solution was found to provide a compatible packet delivery ration in which transmitted packets are examined for any potential attack within nodes. Meanwhile, the proposed solution offered a remarkably less packet drop rate as compared to the work of Ahmed *et al.* (2014). Adaobi *et al.* (2012) stated that packet delivery ratio may results in an increase in packet drops when experiencing denial of service attacks in which a traffic pattern can be observed and compared to other realistic one. The same was addressed by Bensaid *et al.* (2016) who highlighted the association between packet drop rate and time for processing nodes in a network. Based on these, the proposed solution in the present study is believed to offer the necessary antecedents for examining and preventing black hole attack in multiple network nodes.

Future Works

Since this study attempted to provide a reliable solution for improving network performance when experiencing black hole attach, lot of research works are still needed to extend the current understanding of black hole prevention and detection methods. This study was limited to discover and analyze the potential effect of black hole attack in VANETs using AODV protocol only. As such, other VANETs routing protocols can also be examined by future researchers including Temporally Ordered Routing Protocol, Dynamic Source Routing, Connectivity-Aware Routing and others. In addition, future works may consider testing the proposed solution on other types of attacks such as Wormhole, Jellyfish and Sybil attacks.

Acknowledgement

The author is thankful to the reviewers.

Ethics

The author certifies that no actual or potential conflict of interest in relation to this work.

References

Adaobi, O., E. Igbesoko and M. Ghassemian, 2012. Evaluation of security problems and intrusion detection systems for routing attacks in wireless self-organized networks. Proceeding of the 5th International Conference on New Technologies, Mobility and Security, May 7-10, IEEE Xplore Press, pp: 1-5. DOI: 10.1109/NTMS.2012.6208721

Ahmed, E.F., R.A. Abouhogail and A. Yahya, 2014. Performance evaluation of black hole attack on VANET's routing protocols. Int. J. Software Eng. Applic., 8: 39-54.

Alheeti, K.M.A., A. Gruebler and K.D. McDonald-Maier, 2015. An intrusion detection system against malicious attacks on the communication network of driverless cars. Proceedings of the 12th Annual IEEE Consumer Communications and Networking Conference, Jan. 9-12, IEEE Xplore Press, Las Vegas, pp: 916-921. DOI: 10.1109/CCNC.2015.7158098

Al-Kahtani, M.S., 2012. Survey on security attacks in Vehicular Ad hoc Networks (VANETs). Proceedings of the 6th International Conference on Signal Processing and Communication Systems, Dec. 12-14, IEEE Xplore Press, Gold Coast, pp: 1-9. DOI: 10.1109/ICSPCS.2012.6507953

Arya, N., U. Singh and S. Singh, 2015. Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm. Proceedings of the International Conference on Computer, Communication and Control, Sep. 10-12, IEEE Xplore Press, Indore, pp: 1-5. DOI: 10.1109/IC4.2015.7375649

Baiad, R., O. Alhussein, H. Otrok and S. Muhaidat, 2016. Novel cross layer detection schemes to detect blackhole attack against QoS-OLSR protocol in VANET. Vehicular Commun., 5: 9-17.

Bensaid, C., S.B. Hacene and K.M. Faraoun, 2016. Detection and ignoring of black hole attack in vanets networks. Int. J. Cloud Applic. Comput., 6: 1-10. DOI: 10.4018/IJCAC.2016040101

Bibhu, V., R. Kumar, B.S. Kumar and D.K. Singh, 2012. Performance analysis of black hole attack in VANET. Int. J. Comput. Network Inform. Security, 4: 47-54. DOI: 10.5815/ijcnis.2012. 1 1 .0 6

Choure, K. and S. Sharma, 2013. Patterned and protected AODV against black hole, wormhole and grey hole attacks in convalescing routing for Ad-hoc network. Int. J. Comput. Sci. Inform. Security, 11: 1-5.

Dixit, K., K.K. Joshi and N. Joshi, 2015. A novel approach of trust based routing to select trusted location in AODV based VANET: A survey. Int. J. Hybrid Inform. Technol., 8: 335-344.

Djenouri, D., M. Bouamama and O. Mahmoudi, 2009. Black-hole-resistant ENADAIR-based routing protocol for mobile Ad hoc networks. Int. J. Security Netw., 4: 246-262.

Jotangiya, P.U., R. Agrawal and P. Scholar, 2016. An enhance approach of detection and prevention of black hole and gray hole attack on AODV routing protocol over MANET. Int. J. Eng. Sci., 5: 5475- 5477. DOI 10.4010/2016.1339

Kasiran, Z. and S.N. Hassan, 2013. Scalability impact on VANET routing protocols performance. Proceedings of the 3rd International Conference on Electric and Electronics, (CEE'13) Atlantis Press. DOI: 10.2991/eeic-13.2013.50

Kaur, H. and P. Bansal, 2015. Efficient detection & prevention of Sybil attack in VANET. Int. J. Innovative Sci., Eng. Technol., 2: 606-611.

Kaushik, K. and S. Tayal, 2016. Performance analysis of black hole attack in VANET. Int. J. Wired Wireless Communi., 4: 29-34.

Kumar, M. and K. Bhardwaj, 2015. Impact of black hole on AODV based routing in vehicular Adhoc networks. Int. J. Wired Wireless Commun., 4: 1-8.

Lee, B. and E. Jeong, 2016. A black hole detection protocol design based on a mutual authentication scheme on VANET. KSII Trans. Internet Inform. Syst., 3: 1467-1480. DOI: 10.3837/tiis.2016.03.032

Medina, E., D. Lopez, R. Meseguer, S.F. Ochoa and D. Royo, 2016. Mobile Autonomous Sensing Unit (MASU): A framework that supports distributed pervasive data sensing. Sensors, 16: 1-27. DOI: 10.3390/s16071062

Nadeem, A. and M. Howarth, 2013. Protection of MANETs from a range of attacks using an intrusion detection and prevention system. Telecommun. Syst., 52: 2047-2058.

Nafaa, M. and S. Ghanemi, 2014. Analysis of security attacks in AODV. Proceedings of the International Conference on Multimedia Computing and Systems, Apr. 14-16, IEEE Xplore Press, Marrakech, pp: 752-756. DOI: 10.1109/ICMCS.2014.6911193

Pathan, A.S.K., 2016. Security of self-organizing networks: MANET, WSN, WMN, VANET. 1st0 Edn., CRC Press, ISBN-10: 1439819203, pp: 638.

Sharma, S., M.K. Sah and A. Malhotra, 2015. An intersection based traffic monitoring using VANET. Int. J. Comput. Applic., 117: 25-30.

Tyagi, P. and D. Dembla, 2014. A taxonomy of security attacks and issues in Vehicular Ad-Hoc Networks (VANETs). Int. J. Comput. Applic., 91: 22-29. DOI: 10.5120/15893-5040

Varshney, T., T. Sharma and P. Sharma, 2014. Implementation of watchdog protocol with AODV in mobile ad hoc network. Proceedings of the 4th International Conference on Communication Systems and Network Technologies, Apr. 7-9, IEEE Xplore Press, Bhopal, pp: 217-221. DOI: 10.1109/CSNT.2014.50

Zeadally, S., R. Hunt, Y.S. Chen, A. Irwin and A. Hassan, 2012. Vehicular ad hoc networks (VANETS): Status, results and challenges. Telecommun. Syst., 50: 217-241.