ISSN 2278-3091

Volume 8, No.1.2, 2019

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse0481.22019.pdf

https://doi.org/10.30534/ijatcse/2019/0481.22019

WCBAODV: An Efficacious approach to detect Wormhole attack in VANET using CBAODV Algorithm

Arul Kumar[1], Mohammed Gouse Galety[2], Mohammed Nuru[3], Tigist Adam[4]

[1]Assistant Professor of IT, College of Computing, Debre Berhan University, Ethiopia.
[2]Assistant Professor, Department of Computer Network,
Lebanese French University, Erbil, KR-Iraq.
[3]Course Coordinator of IT, College of Computing, Debre Berhan University, Ethiopia.
[4]Dean, College of Computing, Debre Berhan University, Ethiopia.
[1]arulkumar@ieee.org, [2]galety.143@lfu.edu.krd

ABSTRACT

Vehicular nodes in VANET are high energy nodes that can travel randomly to form an Ad-hoc network. These high energy nodes are dynamic in nature and moves more quickly within the network, leading to drastic changes in network topology. Additionally, VANET faces more obstacles and new challenges compared to mobile nodes in MANET. Due to open access atmosphere, vehicular nodes share information with other nearby nodes that are exposed to several security issues. Security attacks in VANET arise because of absence nodes, driver confidentiality and legitimacy. Wormhole attack is one of the major security issues faced by vehicular nodes in VANET. This attack helps the attacker to receive a data packet from one end of the network and redirects that data packet to another. Then, it makes attacker to replay them into the participating network from that end point itself. To solve this issue, the CBAODV algorithm is chosen to detect Wormhole attacks based on the early detection of the characteristics of each vehicular node. Wormhole attack is detected by Route Analysis model and by calculating the Round Trip Time (RTT) in VANET. Compared to other traditional detection techniques in VANET, the proposed WCBAODV algorithm performs better for secure VANET communication. In order to simulate and analyze the results, the NS2 simulator is used to design and examine the VANET environment.

Keywords: CBAODV, Wormhole attack, VANET, NS2, Route Analysis, Round Trip Time, Malicious Node

1. INTRODUCTION

VANET are important for providing the Ad-hoc services by using Intelligent Transport (IT) systems. The main aim to provide safe driving environment by sending some alert message to neighbor vehicular nodes. The alert messages are broadcasted when there is any suspicious change in the network environment. Each vehicle can communicate with other vehicle to forward messages as V2V model. Road Side Terminals (RSTs) are the fixed Ad-hoc nodes placed at the end of each street to support V2V communication and this model is referred as V2I. RSTs are provided with internet facilities to perform route backup at the remote server and this is stated as I2I communication [1].

In order to disturb the communication in VANET several security attacks are performed by attackers to steel the information by sending malicious data packets. Wormhole attack is made by attackers by making themselves as a trustable intermediate node in the network. In this attack, malicious nodes make a “Tunnel” mechanism for redirecting the packets to the desired destination node. Then, data packets are sent by using these malicious nodes to the targeted node. The malicious nodes created by the attackers plays a major role when compared to trustable nodes during data broadcasting [2]. So, Wormhole attack is a very a challenging task to handle vehicular nodes in VANET environment.

In literature, the CBAODV algorithm is used to avoid connection breakage in VANET by using the RSTs [3]. RSTs analysis each data packet and stores in its routing information before forwarding to the vehicular node. In order to detect Wormhole attack, the existing CBAODV algorithm is chosen as a best model to strengthen this research work. This method to detect Wormhole in VANET by using CBAODV algorithm and it is named as WCBAODV. In this paper, WCBAODV algorithm is proposed to detect the occurrence of Wormhole attack by Route Analysis model and calculating the Round Trip Time. This paper is organized as follows: Section 2 presents related works of Wormhole attack. Section 3 gives a description of the proposed WCBAODV algorithm. Section 4 explains the methodology used in creating WCBAODV algorithm. Performance analysis of WCBAODV is carried out with AODV algorithm and it is represented as graphs in Section 5. Section 6 gives an overall summary and limitation of the proposed WCBAODV algorithm.

2. RELATED WORKS

Patel et. al. proposed a Wormhole detection mechanism in Wireless Sensor Networks. This detection mechanism is based on neighborhood information and alternate path length calculation [4]. Verma P et. al., developed an Agent-based

Wormhole attack detection and prevention algorithm in Cloud network using MapReduce Technique [5]. Multiple agent nodes by using the IDS are utilized for analyzing the behavior of nodes to calculate the traffic in the network. Hop count, data packet path and time delay are taken into consideration for analyzing the traffic. MapReduce technique is used to process the data using the key values for analyzing the traffic. The IDs of the malicious nodes are informed by nearby nodes in the Cloud environment. Similar technique is discussed in [25].

Kartigadevi et. al., designed a Wormhole detection and prevention mechanism using the EIGRP protocol [6]. This model is developed based on the Round Trip Time calculation in Wireless Sensor Networks. In order to detect malevolent node, shortest route and round trip time difference are used in this research work. Harsnyi K et. al., introduced a Wormhole attack detection approach using Spanning trees in Wireless Sensor Networks (WSN) [7]. The affected sensor by Wormhole attacks are identified by this model in WSN. This design is developed by calculating the connectivity information of the network design.

Rmayti et. al., proposed a Wormhole detection technique using Graph based model in MANETs [8]. Shortest path is calculated to check whether a node is undergone a Wormhole attack or not. This Wormhole tunnel reduces significantly the length of the paths passing through it. Majumder et. al., developed a Wormhole detection technique using absolute deviation statistical approach in MANET [9]. An Absolute Deviation of statistical approach is used to avoid and to prevent Wormhole attack in MANET. It is found that Absolute deviation covariance and correlation take less time to detect Wormhole attack than classical one. Proposed design performs better than existing technique AODV. MATLAB simulator is used for performance analysis. Packet drop pattern is also measured for Wormholes using Absolute Deviation Correlation Coefficient.

3. DESCRIPTION OF WCBAODV

The challenging aspect of Wormhole attack in Ad-hoc creates a “tunnel” and acts as a trustable node in network with more broadcasting capacity. This Wormhole attack creates a fake route using a malicious node and redirects the data packets to desired location in the network. To control the entire network or communication, these malicious nodes act as a nearby neighbor node and forwards the original data packets to targeted node.

Route analysis is not done by the participating nodes to predict the nature of the nodes [10]. It gives a chance for the attackers to perform Wormhole attacks to redirect the nodes to unknown location. So, it is not an easy task to find the nature of malicious node in the network. Finally, the malicious node will not forward the data packets but it will drop or redirects the data packets which makes the service to be unavailable or denied. In order to detect the malicious node which causes Wormhole attack, VANET needs some special techniques like Route Analysis and Round Trip Time calculation.

Route Analysis

Route Analysis is done to identify the strength of the route between the two nodes in the network. Calculating the strength of the route helps to strengthen the route quality between the nodes [11]. Due to high mobility of nature vehicular nodes in VANET creates the breakage in the communication which leads to weakness of the route between the nodes. Source node send the Route Request (RREQ) data packet to the nearby nodes to find the destination node. Then, Destination node sends the Route Reply (RREP) data packet as a reply to the Source node. Route strength is identified based on Route Analysis by using,

$Route\ Strength\ (RS) = Time_{min}\ (NNC_{T1}, N_{x-1}, N_x)$

Here, NNC_{T1} is the time taken to connect with Neighbor Node Connection. N_{x-1}, N_x is the distance between the nodes during data transmission.

$Occurrence\ of\ Route\ Used\ (Route_{Max}) = (NRT_{Max\_Time} / NR_{Max\_Route})$

Here, RST calculates the maximum number of time a route is used for sending and receiving the data packets is calculated based on the above formula. NRT_{Max_Time} is the maximum number of times a route is used by a node for data transfer. NR_{Max_Route} is the total number of Route available in the network between the sender and receiver I the network [12].

Round Trip Time (RTT)

Round Trip Time defines the total time taken by a sender to send RREQ and to receive for a RREP from the destination node [13]. For example in the Figure 1, Source Node communicates with RST and RST will forward the data packet to the destination node. The formula to calculate RTT is,

$$Round\ Trip\ Time\ (RTT) = Source\_RST(T_1+T_2) + RST\_Destination(T_3+T_4)$$

Here, $Source\_RST(T_1+T_2)$ is the total time taken to send RREQ from Source to RST and to receive RREP from RST to Source node. $RST\_Destination(T_3+T_4)$ is the total time taken to send a RREQ from RST to Destination and to receive RREP from Destination to RST.

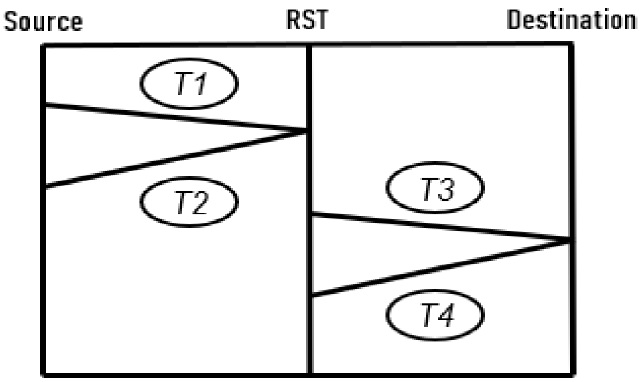

Figure 1: RTT calculation between Source and Destination

Calculating RTT is very useful when determining the distance and route strength between the two nodes. This is commonly useful to calculate the delay and the reliability to send RREQ and to receive RREP.

For example, based on the Figure 1, RREQ is sent for 5 times from Source node to Destination node and RREP is received for 5 times from Destination node to Source node. The time taken by each RREQ for each Round Trip Time (RRT) is given below.

$RREQ_1 = 16.822, RREQ_2 = 17.604, RREQ_3 = 16.904, RREQ_4 = 16.929, RREQ_5 = 16.144$

Based on the RTT value, the RST will generate the following statistic information as in Table 1. These values are stored in the routing information of RST to detect the malicious node. When the time taken by a RREQ is abnormal means, then RST will identify the node as a malicious node. Later, RST will blacklist the node and that node is removed from the routing information.

Table 1: Round Trip Time Statistics

Segment	Round_TripMin	Round_TripMax	Round_TripAvg	Round_TripDev
1	16.144	16.881	17.604	0.463

Here, $Round\_Trip_{Min}$ is the Minimum time taken for a round trip, $Round\_Trip_{Max}$ is the maximum time taken for a round trip, $Round\_Trip_{Avg}$ is the average time taken for a round trip, $Round\_Trip_{Dev}$ is the standard deviation of time taken during the round trip [14, 15].

The Round Trip Time between the Source and Destination node varies depends on the following factors [16]:

- Energy of a Source Node
- Link Quality between Source and Destination
- Number of nodes in the network
- Amount of traffic between the Source and Destination
- Number of Requests handled by the RSTs
- Speed and Direction of travel of a node
- Occurrence of interference in the network

4. WCBAODV ALGORITHM

The proposed WCBAODV algorithm is designed effectively to detect malicious node in VANET with the help of RST by calculating Route Analysis and Round Trip Time. The proposed WCBAODV algorithm is given below.

```
Step 1: Let the Source Node (SN) sends Route Request as RREQ
Step 2: RST receives the RREQ and forwards to Nearby Node
Step 3: Nearby Node forwards RREQ to Destination Node (DN)
Step 4: Destination Node replies with RREP
Step 5: RST receives the RREP and updates its Routing information
    RST calculates the Route Strength
        Route Strength (RS) = $Time_{min} (NNC_{T1}, N_{x-1}, N_x)$
    RST calculates the Maximum Occurrence of the Route
        Occurrence of Route Used ($Route_{Max}$)= ($NRT_{Max\_Time}$/ $NR_{Max\_Route}$)
    RST calculates the Round Trip Time (RTT)
        Round Trip Time (RTT) = Source_RST($T_1+T_2$) + RST_Destination($T_3+T_4$)
Step 6: if (RTT< $Round\_Trip_{Min}$) and ($Route_{Max}$>Maximum) then
    RST detects the Route as Malicious Route
    RST sends fake RREQ to detect Malicious Node
    RST receives fake RREP from the Malicious Node
    RST confirms the Malicious Node
    RST removes the Malicious Node from its Routing Table
    RST informs about the Malicious Node to other nodes
    RST updates its Routing table
Step 7: RST forwards RREP to Source
Step 8: Source communicates with Destination using RST
```

In the proposed WCBAODV algorithm, Source Node (SN) sends a RREQ to reach Destination Node (DN). RST acts as an intermediate node between Source and Destination node. RST receives the RREQ from the Source Node and forward to the nearby neighbor node. Neighbor node forward the received RREQ to the destination node in the network. Destination node in the network receives the RREQ and makes a reply by sending a RREP to the Source Node. RST updates its routing information before forwarding the RREP to the Source Node. At this stage, RST performs Route Analysis by calculating the Route Strength (RS), Maximum occurrence of the route ($Route_{Max}$) and Round Trip Time. RST creates a RTT table by using $Round\_Trip_{Min}$, $Round\_Trip_{Max}$, $Round\_Trip_{Avg}$ and $Round\_Trip_{Dev}$. RST detects the route as malicious route when the *(RTT*< $Round\_Trip_{Min}$) and *($Route_{Max}$>Maximum)* and RST confirms and marks the route as malicious route. Otherwise, RST simply forwards the RREP to Source node. This malicious route is informed by broadcasting this information to the nearby nodes by RST. After updating its routing information, RST forwards the RREP to source. Finally, Source Node communicates with the Destination using the updated routing information in RST.

5. PERFORMANCE ANALYSIS OF WCBAODV

For experimental setup in WCBAODV, NS2 simulator is used to analyze the QoS parameters like Packet Delivery Ratio, End to End Delay and Throughput. Packet Delivery Ratio (%) defines the ratio of delivery of the data packet from source to destination without loss. End to End Delay (Sec.) describe the delay occurred in sending a data packet from source node to destination node. Throughput (Bits/Sec.) outlines the number of successful delivery of data packets in a certain period of time. The proposed WCBAODV algorithm in compared with the existing CBAODV algorithm with respect to number of nodes like 8, 16, 32 and 64 in a network. Simulation Parameters used for this experimental setup is given in Table 2.

Table 2: Simulation Parameters

Parameter	**Value**
Tool	NS2.25
Data Packet	512 bytes
MAC Type	MAC / 502.11
Channel Type	Channel / Wireless
Movement	Random Waypoint
Network Interface Type	Phy / Wireless Phy
Interface Queue Type	Queue / Drop Tail / PriQueue
Routing Protocol	CBAODV and WCBAODV
Radio Propagation	Two Way Ground
Channel and Capacity	Wireless 10 Mb/s
Buffer Size	1000 Packets
Number of Nodes	8, 16, 32, 64
Simulation Time	200s
Range of Transmission	230m
Traffic Rate	CBR
Simulation Area	500m x 500m

Initially, the simulation results of normal AODV algorithm are noted based on simulation parameters for 8, 16, 32 and 64 nodes respectively. Next, the malicious nodes are added in the same environment without making any changes in the network to collect the results again. At last, the proposed WCBAODV algorithm is implemented to secure the VANET for the given scenario.

The Figure 2, represents the initial setup of a VANET environment with 8 nodes namely, 0, 4, 3, 7, 2, 1, and 8. Here, Node 0 is considered as Source node and Node 8 is the Destination Node for the data transmission.

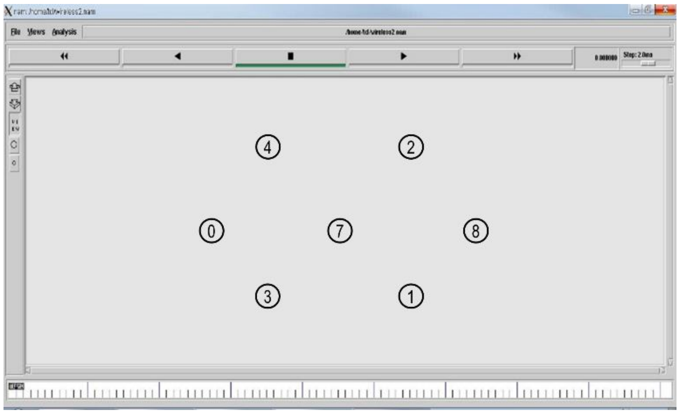

Figure 2: Initial Setup of VANET environment

In Figure 3, by calculating the Route Analysis and Round Trip Time, Node 7 is identified as a malicious node which cause Wormhole attack. Later, this Node 7 is blacklisted by RST and it noticed to all other nodes in the network.

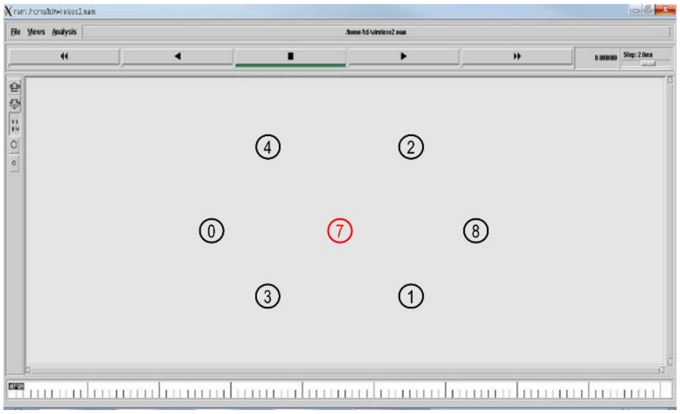

Figure 3: Malicious Node in Wormhole attack

In Figure 4, 5 and 6, the X-axis is the number of node and Y-axis is the parameters for the routing protocols. In Figure 4, the Throughput (Bits/Sec) of AODV vs. WCBAODV is calculated by varying the number of nodes in VANET as 8, 16, 32, 64 respectively.

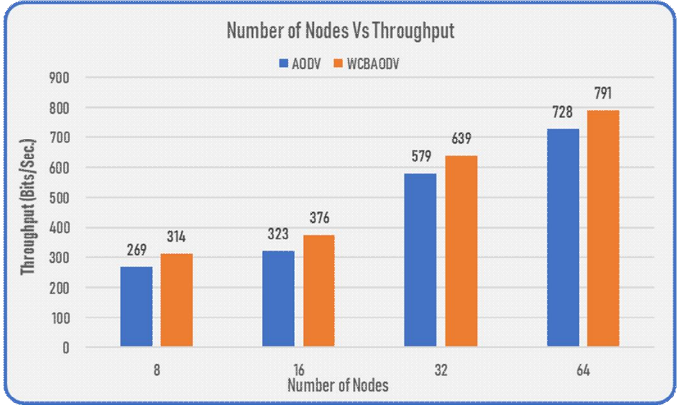

Figure 4: Throughput (Bits/Sec.) Analysis of AODV vs WCBAODV

In Figure 5, Packet Delivery Ratio (%) of AODV vs. WCBAODV is calculated by varying the number of nodes in VANET as 8, 16, 32, 64 respectively.

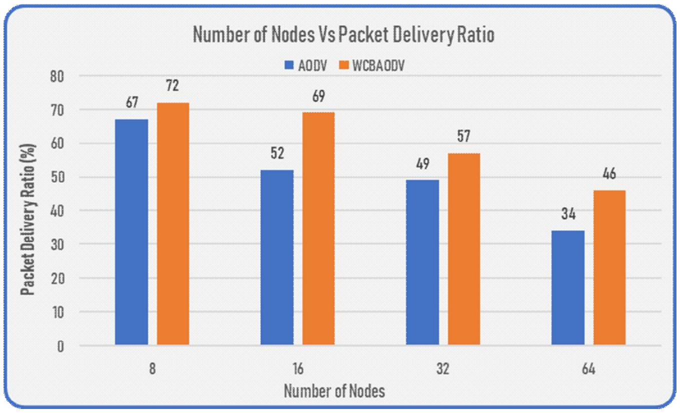

Figure 5: Packet Delivery Ratio (%) Analysis of AODV vs WCBAODV

In Figure 6, End to End Delay (Sec.) of AODV vs. WCBAODV is calculated by varying the number of nodes in VANET as 8, 16, 32, 64 respectively.

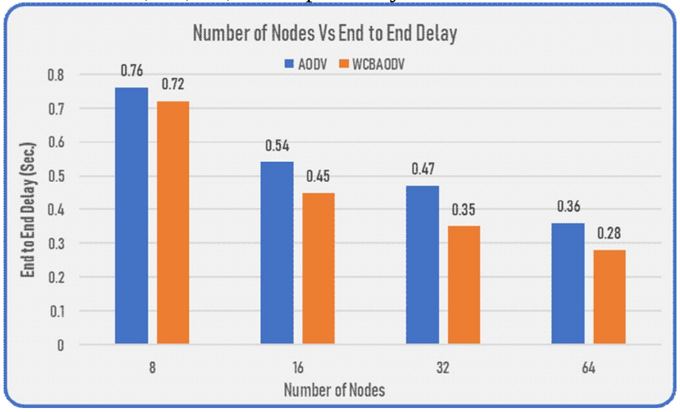

Figure 6: End to End Delay (Sec.) Analysis of AODV vs WCBAODV

WCBAODV Findings and Interpretation

Figure 4 shows the values of average Throughput (Bits/Sec.) generated for AODV and WCBAODV for the nodes 8, 16, 32 and 64. The variance in the throughput value for the proposed WCBAODV increases as the number of nodes increases by calculating the Route analysis and Round Trip Time. For an instance, when the number of nodes is 6, Throughput (Bits/Sec.) of WCBAODV is 324 but AODV is 269 only.

In Figure 5, values of Packet Delivery Ratio (%) is given by comparing with AODV and WCBAODV for the nodes 8, 16, 32 and 64. The number of packets delivered increases when the number of nodes increases in the network. Here, WCBAODV delivers a greater number of data packets from Source to Destination when compared to existing AODV algorithm. For an illustration, the Packet Delivery Ratio (%) of WCBAODV has greater value of 72 (%) for 6 nodes but the AODV has only ratio of 67 (%) only.

In Figure 6, AODV algorithm increases the average End to End Delay in the network due to malicious nodes. But, the End to End Delay decreases when implementing the WCBAODV in the same environment without making changes in simulation environment. These values show that the average End to End Delay is increased when the number of nodes increased as 8, 16, 32 and 64. For example, when the number of nodes is 6, End to End Delay (Sec.) of AODV is 0.76 (Sec.) but WCBAODV is 0.72(Sec.) only.

6. CONCLUSION

In this paper, a new algorithm called WCBAODV is proposed to detect Wormhole attack in VANET by using Route Analysis and Round Trip Time concepts. RSTs are effectively used for detecting the malicious nodes. Here, malicious nodes are identified and blacklisted to avoid packet drops. RSTs play a major role to identify the malicious and to protect the genuine nodes in VANET. By considering the Route Analysis and Round Trip Time in VANET, End to End Delay (Sec.) values are decreased. In addition, the Packet Delivery Ratio (%) and Throughput (Bits/Sec.) values are increased with the help of RSTs in WCBAODV algorithm.

Limitation of WCBAODV

Even though, the proposed WCBAODV algorithm detects the malicious nodes that cause Wormhole attack in VANET, the other parameters apart from Hop Count [17], Route Categorization [18] and Route Prioritization [19, 20] techniques are not measured. Route Analysis and Round Trip Time is calculated with the help of RSTs. This approach will fail when RSTs becomes idle due to energy efficiency issue.

REFERENCES

[1] Ratnasih, R., Perdana, D., Wulandari, T., & Pratama, M. I. (2018). **Performance Analysis of Reactive Routing Protocol on VANET with Wormhole Attack** Schemeaper. JURNAL INFOTEL, 10(3), 138-143. https://doi.org/10.20895/infotel.v10i3.384

[2] Abdulkader, Z. A., Abdullah, A., Abdullah, M. T., & Zukarnain, Z. A. (2018). **Malicious node identification routing and protection mechanism for vehicular ad-hoc network against various attacks**. International Journal of Networking and Virtual Organisations, 19(2-4), 153-175. https://doi.org/10.1504/IJNVO.2018.095419

[3] Arulkumar, N., & Raj, E. G. D. P. (2015). **CBAODV: An enhanced reactive routing algorithm to reduce connection breakage in VANET**. In Artificial Intelligence and Evolutionary Algorithms in Engineering Systems (pp. 533-539). Springer, New Delhi. https://doi.org/10.1007/978-81-322-2135-7_57

[4] Patel M., Aggarwal A., Chaubey N. (2019) **Detection of Wormhole Attack in Static Wireless Sensor Networks. In: Bhatia S., Tiwari S., Mishra K., Trivedi M**. (eds) Advances in Computer Communication and Computational Sciences. Advances in Intelligent Systems and Computing, vol 760. Springer, Singapore https://doi.org/10.1007/978-981-13-0344-9_39

[5] Verma P., Tapaswi S., Wilfred Godfrey W. (2018) **Agent-Based Wormhole Attack Detection and Prevention Algorithm in the Cloud Network Using**

MapReduce Technique. In: Saeed K., Chaki N., Pati B., Bakshi S., Mohapatra D. (eds) Progress in Advanced Computing and Intelligent Engineering. Advances in Intelligent Systems and Computing, vol 564. Springer, Singapore https://doi.org/10.1007/978-981-10-6875-1_43

[6] Karthigadevi, K., Balamurali, S., & Venkatesulu, M. (2018). **Wormhole Attack Detection and Prevention Using EIGRP Protocol Based on Round Trip Time**. *Journal of Cyber Security and Mobility*, *7*(1), 215-228.

[7] Harsányi, K., Kiss, A., & Szirányi, T. (2018, January). **Wormhole detection in wireless sensor networks using spanning trees**. In *Future IoT Technologies (Future IoT), 2018 IEEE International Conference on* (pp. 1-6). IEEE. https://doi.org/10.1109/FIOT.2018.8325596

[8] Rmayti, M., Begriche, Y., Khatoun, R., Khoukhi, L., & Mammeri, A. (2018, February). **Graph-based wormhole attack detection in mobile ad hoc networks (MANETs)**. In *Mobile and Secure Services (MobiSecServ), 2018 Fourth International Conference on* (pp. 1-6). IEEE. https://doi.org/10.1109/MOBISECSERV.2018.8311439

[9] Majumder, S., & Bhattacharyya, D. (2018, January). **Mitigating wormhole attack in MANET using absolute deviation statistical approach**. In *Computing and Communication Workshop and Conference (CCWC), 2018 IEEE 8th Annual* (pp. 317-320). IEEE. https://doi.org/10.1109/CCWC.2018.8301780

[10] Kulla, E., Morita, S., Katayama, K., & Barolli, L. (2018, July). **Route Lifetime Prediction Method in VANET by Using AODV Routing Protocol (AODV-LP)**. In Conference on Complex, Intelligent, and Software Intensive Systems (pp. 3-11). Springer, Cham. https://doi.org/10.1007/978-3-319-93659-8_1

[11] Nabil, M., Hajami, A., & Haqiq, A. (2019). **Predicting the Route of the Longest Lifetime and the Data Packet Delivery Time between Two Vehicles in VANET**. Mobile Information Systems, 2019. https://doi.org/10.1155/2019/2741323

[12] AlFarraj, O., Tolba, A., Alkhalaf, S., & AlZubi, A. (2019). **Neighbor Predictive Adaptive Handoff Algorithm for Improving Mobility Management in VANETs**. Computer Networks. https://doi.org/10.1016/j.comnet.2019.01.020

[13] de Sousa, A. M., RC, F. A., & Sampaio, L. N. (2018). **A Link-Stability-Based Interest-Forwarding Strategy for Vehicular Named Data Networks**. IEEE Internet Computing, 22(3), 16-26. https://doi.org/10.1109/MIC.2018.032501512

[14] Duan, M., Zhang, C., Li, Y., Xu, W., Ji, X., & Liu, B. (2018, October). **Neighbor Cache Explore Routing Protocol for VANET based on Trajectory Prediction**. In 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC) (pp. 771-776). IEEE. https://doi.org/10.1109/IAEAC.2018.8577903

[15] Al-Mutiri, R., Al-Rodhaan, M., & Tian, Y. (2018). **Improving Vehicular Authentication in VANET**, International Journal of Communication Networks and Information Security (IJCNIS), 10(1).

[16] Pasin, M., Seghrouchni, A. E. F., Belbachir, A., Peres, S. M., & Brandao, A. A. F. (2018, July). **Computational Intelligence and Adaptation in VANETs: Current Research and New Perspectives**. In 2018 International Joint Conference on Neural Networks (IJCNN) (pp. 1-7). IEEE. https://doi.org/10.1109/IJCNN.2018.8489689

[17] Kchaou, A., Abassi, R., & El Fatmi, S. G. (2018, November). **A New Trust based Routing Protocol for VANETs**. In 2018 Seventh International Conference on Communications and Networking (ComNet) (pp. 1-6). IEEE. https://doi.org/10.1109/COMNET.2018.8621921

[18] Latif, S., Mahfooz, S., Jan, B., Ahmad, N., Cao, Y., & Asif, M. (2018). **A comparative study of scenario-driven multi-hop broadcast protocols for VANETs**. Vehicular Communications. https://doi.org/10.1016/j.vehcom.2018.01.009

[19] Tahmasebi, M., & Khayyambashi, M. R. (2018). **An efficient model for vehicular cloud computing with prioritizing computing resources**. Peer-to-Peer Networking and Applications, 1-10. https://doi.org/10.1007/s12083-018-0677-6

[20] García-Magariño, I., Sendra, S., Lacuesta, R., & Lloret, J. (2018). **Security in vehicles with IoT by prioritization rules, vehicle certificates and trust management**. IEEE Internet of Things Journal. https://doi.org/10.1109/JIOT.2018.2871255