Anil Chaudhary · Chothmal Choudhary ·
Mukesh Kumar Gupta · Chhagan Lal ·
Tapas Badal *Editors*

Microservices in Big Data Analytics

Second International, ICETCE 2019, Rajasthan, India, February 1st-2nd 2019, Revised Selected Papers

Springer

Microservices in Big Data Analytics

Anil Chaudhary · Chothmal Choudhary ·
Mukesh Kumar Gupta · Chhagan Lal ·
Tapas Badal
Editors

Microservices in Big Data Analytics

Second International, ICETCE 2019,
Rajasthan, India, February 1st-2nd 2019,
Revised Selected Papers

Springer

Editors
Anil Chaudhary
Department of Information Technology
Swami Keshvanand Institute of Technology
Jaipur, Rajasthan, India

Mukesh Kumar Gupta
Department of Computer Science
and Engineering
Swami Keshvanand Institute
of Technology
Jaipur, Rajasthan, India

Tapas Badal
Department of Computer Science
and Engineering
Swami Keshvanand Institute
of Technology
Jaipur, Rajasthan, India

Chothmal Choudhary
Department of Computer Science
and Engineering
Swami Keshvanand Institute
of Technology
Jaipur, Rajasthan, India

Chhagan Lal
Postdoctoral Research Fellow
University of Padua
Padua, Italy

ISBN 978-981-15-0127-2 ISBN 978-981-15-0128-9 (eBook)
https://doi.org/10.1007/978-981-15-0128-9

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Preface

The 2nd International Conference on "Emerging Technologies in Computer Engineering: Microservices in Big Data Analytics" (ICETCE-2019) was held at Swami Keshvanand Institute of Technology, Management and Gramothan (SKIT), Jaipur, Rajasthan, India, on February 1–2, 2019. The main keynote addresses were given by Prof. (Dr.) Arun K. Somani, Associate Dean for Research, College of Engineering, Iowa State University, Ames, USA, and Prof. Seeram Ramakrishna, Vice President, Research Strategy, NUS, Singapore.

We received 253 submissions from all over the world. The technical program committee members carefully selected the papers after peer review process by at least three reviewers. Out of 253 submissions, 29 papers were selected for presentation in the conference and publication in Springer CCIS series, and 16 papers were selected for presentation in the conference and publication in this Springer book.

We wish to thank the management of Swami Keshvanand Institute of Technology, Management and Gramothan (SKIT), Jaipur, Rajasthan, India, for providing the best infrastructure to organize the conference. We are also thankful to DST and AICTE for financial sponsoring of the event. We are also very thankful to Springer for supporting ICETCE-2019. We are also very thankful to Prof. M. N. Hoda, Ms. Suvira Srivastav, and Ms. Nidhi Chandhoke for the approval and continuous help.

We hope that this conference proceeding will prove to be useful.

Jaipur, India

Anil Chaudhary
Chothmal Choudhary

Contents

A Fuzzy Logic-Based Control System for Detection and Mitigation of Blackhole Attack in Vehicular Ad Hoc Network

Ankit Kumar, Pankaj Dadheech, Mahender Kumar Beniwal, Basant Agarwal and Pawan Kumar Patidar

1 Introduction

VANET (Vehicular Ad Hoc Network), is successor of VANET (Vehicular Ad Hoc Network), and, it is developed for improving the transfer of information among different neighbor vehicles and roadside data points by using wireless communication devices incorporated within vehicles. The development of VANET has cleared path for many applications and methods for the betterment of road safety and travelling convenience. VANET has many properties that lacked in VANET, hence making it a better network than its predecessor. Some of the evolution of properties are higher node mobility and better energy-saving methods. We have investigated about some of the modified mechanisms which were developed to overcome the limitations of VANETs. In the present research of ours, we have mainly focused on its application and assessing the vast and possible VANET programs. We have performed only on simulations because it is not possible for us to check its application on actual vehicles on the streets. Now, for VANETs, we have to try new simulation strategy because the parameters used for VANET gave us non-precise values. One of the possible strategies is to create mobility traces of vehicles by the help of traffic simulation,

A. Kumar (✉) · P. Dadheech · M. K. Beniwal · B. Agarwal
Swami Keshvanand Institute of Technology, Management & Gramothan, Jaipur, Rajasthan, India
e-mail: iiita.ankit@gmail.com

P. Dadheech
e-mail: pankaj@skit.ac.in

M. K. Beniwal
e-mail: mbeniwal@skit.ac.in

B. Agarwal
e-mail: basant@skit.ac.in

P. K. Patidar
Poornima College of Engineering, Jaipur, Rajasthan, India
e-mail: pawanlata143@gmail.com

A. Chaudhary et al. (eds.), *Microservices in Big Data Analytics*,
https://doi.org/10.1007/978-981-15-0128-9_15

(network-centric) like SUMO and to use it as input signal for our network simulator, for example, NS2 for simulating the results.

VANET applications can be mainly divided into two categories:

(a) Comfort (Commercial) Applications: One of the technologies used in VANETS are vehicular WiMAX which is social networking technologies with wide applications. Various parameters of performance such as mean throughput and packet loss ratio for the working of VANET incorporating 802.16e are calculated through simulation methods. The simulation model proposed here is almost real because of the feeding of input of the network simulation (NS2) as the data received from the output of the freedom traces for both the instances with the help of traffic simulator (SUMO). These are all predicted keeping in mind the conditions that usually occur in urban scenario for VANET.
(b) Safety-Related Software: VANET is used in many safety-related applications like traffic controller tollbooth management.

2 Related Work

There is lot of work which is already published by different academicians and researchers in the field of VANET, and they also provide solution of security attack possible in VANET. There were lot of researchers and academicians who have taken the help of simulation tool available for simulating the VANET environment to implement the different protocols, and they obtain the result with their proposed solution. The authors [1] offered their work on message authentication in VANET using social network in which they stated that in VANET vehicle shares safety and non-safety information. The motive behind this information is to avoid road accident by alerting driver about the hazards. In this paper, the authors proposed their algorithm in which social network is used to create topology. Message authentication is achieved by using quick response code technique to send profile of user. The authors conclude that through this method, it increases the performance of the system as it uses QR code in message encryption and decryption. The author [2] offered their work on study of Sybil attack on vehicular network in which he stated that security and safety of message are important for vehicular network. Privacy and security of the message motivate strong network design. In this paper, the author presents network threats that can exploit working of VANET and also presents performance comparison of routing protocol in the presence of Sybil. After analysis and survey, the author concluded that ad hoc on-demand distance vector routing protocol works better in network in the presence of attack. The author [3] offered their work on performance analysis of enhanced authentication scheme on VANET using rekey in which he stated that in vehicular ad hoc network on the road there may be chances that some intruders enter into network and affect the normal working of VANET. It requires an authentication mechanism that restricts the entry of malicious node in the VANET. In this paper, the

author proposed enhanced intermediary re-encryption algorithm that reduces overhead packet in the VANET. Through this algorithm, it reduces jitter and delay and increases packet delivery ratio and throughput by restricting attacks in the network. The author concluded by his new method EIRE that the probability of attacks will be reduced in VANET. The authors [4] presented their paper on the security issue on VANET. The authors in their paper said that due to the characteristics of VANET like mobility, no infrastructure, and partition in network, it possesses security threats and hence the security mechanisms which are used to secure networks cannot be used to secure it. The authors propose to explain as well as scrutinize the safety developments of network. The authors said that the VANET technology is very useful and can be used for exchanging information over network of event that is taking place in the surroundings or about to take place like accidents; this type of prior information is very useful to the drivers because it is helpful in road safety. The communication is either V2V or V2I. The environment in vehicular ad hoc network comprises infrastructure and ad hoc. In infrastructure, the nodes in the network are fixed permanently and deployed by government. Bodies but in ad hoc the nodes in network are not fixed, and the connection is initiated by vehicles in the network. The authors further proposed the needs of security in the network such as authentication, non-repudiation, confidentiality, availability, privacy, and identification. The authors also studied about the attacks which can be achieved if these needs are not fulfilled. The authors further studied about the existing solution which is used to secure the network. The authors concluded that VANETs have vast opportunity in the present scenario. They suggested that new mechanisms are needed to be implemented to secure the network; also, they said that a new comparative framework is needed to evaluate many different existing protocols to secure network. The authors [5] presented a review paper to discuss how to discover and separate the harmful node in VANET. The authors said that VANET is a promising technology which can do wonders if put in use and also if its threats can be overcome. It possesses a risk in a network because of its character. The authors in their paper discuss the recent scenario of vehicular ad hoc network. They discuss its working and the security breach that can be done in the network and also the possible solution which are implemented until present to conquer the security breach in the network. They discuss different security attacks like wormhole attack, packet-drop attack, selfish node attack, Sybil attack, DoS attack, DDoS attack, etc. They also discussed the routing protocol which is used in VANET to provide communication between nodes. These protocols are proactive, reactive, and hybrid routing protocol. In proactive, the path of communication is prior known, but in reactive, it is decided dynamically according to the network and situation. Hybrid is the combination of proactive and active routing protocol. The authors concluded that due to the security threat, the network of VANET is defenseless and due to its character, anyone can connect in the network makes the network more defenseless to the attacks. The authors [6] presented their paper on the survey of attack that can be done on VANET; they presented their study on different attack and provide a comparative

study on the attacks and approach to surmount those attacks. The authors said that in the last three or four years, VANET attracts so much attention due to the advantage it provides over network that many researches are around its network and to increase its capacity to use its advantage properly. The authors discussed the desires of security in the network which are needed to make network secure. Further, they discuss the attacks on VANET in detail and provide a habitual as well as restructured approach to surmount that attack. They further categorize these attacks in different classes and provide a comparative study on these attacks. The authors concluded that the attack on VANET is a critical issue because it affects the network and its working. It is sure that it has advantages, but these advantages and its capacity cannot be used properly if these security breaches are not resolved. The authors [7] presented their paper on the analysis of trust-based routing via AODV to find a genuine location in the network. They presented a comparative study on the basis of different study of researches they have done to complete their assessment. The authors discussed that VANET is a mechanism which provides a method to converse different nodes in a momentary network because nodes can connect and disconnect themselves when there is no need to converse. They can share warning and messages about network if it is smooth and overcrowded or if there is a clash in the network, which saves time, increases the competence, provides path protection, and travels organization. Due to these qualities, VANET is a center of attraction in the eyes of many researchers and researches are going on and on to increase its efficiency. The authors in their paper discussed different trust models which are proposed until now and provided a survey about the protocols used for those models. Further, the authors discussed the issues surrounding trust and why trust is necessary to provide a protected and dependable transmission. They discussed the different attacks and how a trust model is helpful to conquer these attacks. The authors concluded that there should be a trust bonding between nodes and their neighbors to make the transmission dependable and protected. The author [8] offered their work on the algorithm to prevent grayhole attack on VANET using multipath approach in which she stated the threats revolving around grayhole and effects of grayhole on VANET. Grayhole attack is one of the security risks in which the traffic is readdressed to such a node that actually does not be real. In this paper, the author proposed routing protocol approach and then discovered the secure pathway in the network by avoiding grayhole attacks. Measurements and calculation are done to determine if network is under attack of grayhole, and then, by routing protocol approach, the author discovered a secure pathway in the network. The author concluded that by her approach the grayhole attack can be avoided in the VANET.

Based on the literature review, we have identified the few attacks which is possible in VANET.

2.1 Attacks on VANET

Many possible attacks are seen in VANET shoots. The main motives for this attack are:

(1) To disrupt network usage for all vehicles.
(2) To promote fake message about the incident in the road.
(3) To steal confidential information (such as using phishing techniques).

There are so many types of attacks possible in VANET, such as the DoS, nodes identifying spoofing, data correction, eavesdropping, man-in-the-middle attack, and timing attack (with time delay attack).

DoS and DDoS Attack The main idea of the DoS attack [9] is deliberately based on prevention of network communication from the next. It is difficult to defend against such attacks, especially in different ways because it can be done in a variety of ways. There are two main strategies for conducting DoS attacks in the workshop add-on networks:

Sybil Attack: Violated security needs: authentication. In the VANET, Sibyl attacks spoof the identity of a single network node with many bogus vehicles (actually nonexistent) and flood the network with incorrect information. The attacker node sends multiple copies of packet in the network of the same work (with false information) using unique fake identities in each alert message. As a result, many messages from different senders can be a serious threat to this dirty when single node forces other vehicles to accept wrong messages.

Sending Bogus Information Infringement Security Requirement, Data Verification, Data Integrity. In this attack, nodes provide incorrect information; there are three types of attacks on other networks (nonexistent), traffic jams, accidents, or off-road suggestion to choose:

(a) The network frames are created or modified; the malicious node enters the network with newly created frames or changes the existing frames with the corrupted slang.
(b) A reconstructed network frame (replay attack) this attack depends on the interaction (raw frame) capture on the VANET and subsequently injects the network. A prominent example of using this attack is the repeated packet sent by ambulance to get a quick ride.
(c) Confusing car sensor (rare attack), the difference between the previous methods is that the confusion attack changes new information or creates existing network frames, not based on the false information injection on the network. This concept depends on the movement of car sensors, which can lead to the generation of specific messages and send them to the network (such as the car involved in accidents and bad weather).

Man-in-the-Middle (MitM) Attacks Violated security requirements: Integrity of information, privacy. This attack [10] depends on the disguise and correction of the

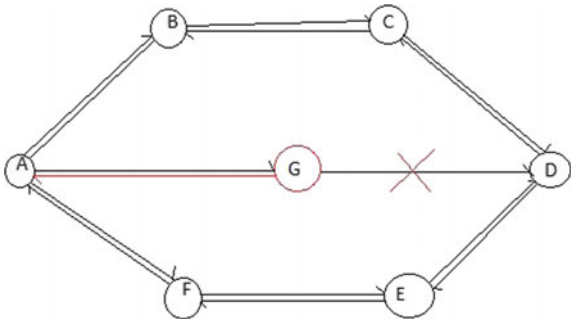

Fig. 1 Packet-drop attack

network traffic. There is usually no significant difference between attack between WANETs and wired networks. The sending of this attack and conflicting network protection cannot seriously affect the information.

Blackhole Attack in VANET VANET has many advantages, and it also possesses threats in its network. In blackhole attack, malicious node through its routing protocol shows in the network that it has shortest route available for communication [11]. Network has a tendency to find the shortest route to transfer messages over network rapidly, and the attacker node shows that it has shortest route available. When the original node requests for the routes to communicate in the network, the attacker node shows that it has new routes available that will provide shortest path to the destination and that provide as a trap once the route is considered for the communication. Now, it is on node to either drop all the packets or transfer it to unknown or may be known node. It is also known as packet-drop attack.

Figure 1 shows how blackhole attack is achieved in the network. Suppose that node "A" wants to transfer message to node "D", then the route should be A–B–C–D or A–F–E–D. But, when node "A" requests for the route, an attacker node, node "G" intercepts the request message, and before the other nodes send response, the attacker node shows that it has the new route which is shortest to the destination. Now, node "A" will consider this path and reject other response of the nodes. Node "G" can transfer the packet to unknown path or can drop the packet. There are two types of packet-drop attack: external and internal packet-drop attack.

External Packet-drop Attack In this type of attack [12], the attacker nodes stay outside the network and reject the access of the processing of the network or generate the obstruction in network which make the network difficult to communicate.

Internal Packet-drop Attack In this type of attack [3], attacker node is practically inside the network and participates in the processing of network. Whenever it sees the opportunity to attack in the network, it shows that it has fresh path which is shortest to destination. Internal attack is more dangerous than external attack.

2.2 *Fuzzy Logic and Fuzzy Sets*

Fuzzy logic is one of the methods that are used for modeling or determining uncertainty. In past few decades, fuzzy logic [13] has grown tremendously in terms of number of applications and popularity.

Fuzzy logic system such as computing and the fuzzy logic controller are based on computation of fuzzy sets. As it is not possible to study in detail all sources of uncertainty for all applications for fuzzy logic controller, but some of the sources of uncertainty are explained in the literature and which are also widely accepted:

(a) High level of noises from various sources affects the input uncertainties as sensor measurement in fuzzy logic controller. In addition, the conditions of environment such as sunshine, wind, and rain can affect the input sensor.
(b) Due to environmental changes, wear, tear, etc., lead to change in actuator that causes uncertainties in control output.
(c) For generating an output, the members and forms of these rules are exposed to uncertainties; depending upon application, these rules are original.

3 Proposed Work

We have proposed an association-based route selection technique to apply over AODV routing protocol to improve the security of the network as well as selecting the shortest path between source node (S) and the destination node (D) on the basis of the trust values of the nodes. Here, we have characterized nodes into three groups on the basis of the changing behavior [14] of nodes. We have shown below three different values of the nodes (Fig. 2).

Here, we have created membership function for tree types of nodes. Like we have created a graph with the boundaries condition like when the value lies between 0 and 1, i.e., $x = 1$, then the trust value is 0.3 and the node is considered as bad node.

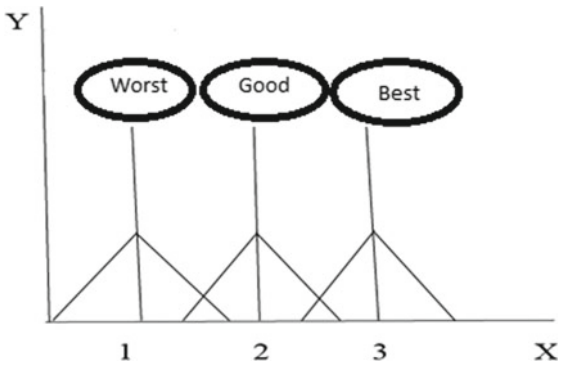

Fig. 2 Types of nodes classified using FBC

In the same way, we have defined the membership value of all the nodes like worst, good node, best node which membership value of node varies from 0 to 1. Here, I have defined three different ranges for the three different nodes:

A node is considered as worst, if X = 0 to X = 1.75 with Y = 0 to Y = 1.
A node is considered as GOOD node, if X = 1.25 to X = 2.75 whose membership value lies between Y = 0 to Y = 1.
A node is considered as best, if X = 2.25 to X = 3.75 whose membership value lies between Y = 0 to Y = 1.

3.1 Calculation of Association Between the Neighboring Nodes in VANET

In a VANET, the association parameter of node P and Q will be as follow:
Worst Node

- Node P did not send or receive any packet from the node Q; then, the trust value between the node P and Q is very low.
- Based on the trust value, the probability of malicious node is very high.
- Newly arrived nodes or the nodes with the malicious behavior are placed under this group.

Known Node

- Node P and node Q transmit some message to each other.
- Trust level between node P and Q is neither too low nor high.
- Probability of being malicious node is expected.

Good Node

- Node P has sent or received large number messages to or from node Q
- Trust level between node P and Q is very high.
- Probability of being malicious node is almost nil.

The above association can be represented with the help of an association table which is a part of all nodes in a vehicular ad hoc network.

The association table for node 1 in Fig. 3 is given (Table 1).

3.2 Association Estimation Technique

The status of association depends upon the trust values. Using the following parameters, the trust values of the nodes are calculated. We have proposed for calculating the trust values between any two given nodes in a network.

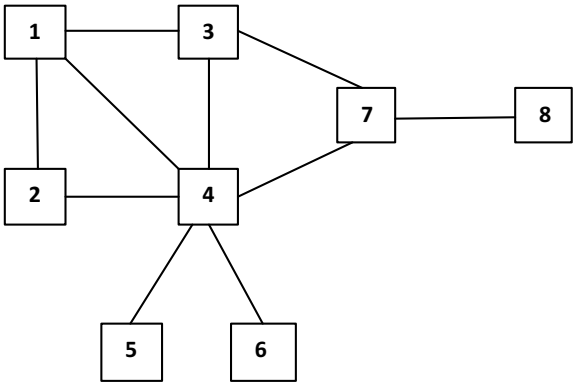

Fig. 3 Nodes in vehicular ad hoc network

Table 1 Node 1 association table

Neighbors	Nature of association
1	Good
2	Good
3	Known
5	Good
7	Bad

$$\text{Trust Value} = \tanh(\text{N1} + \text{N2} + \text{Ack})$$

where N1 = No. of packets neighbour node successfully forwarded/Total no of packet neighbour node has to forward.

In the above expression, if denominator is not equal to zero (=0) and N1 is less than 1 (N1 < 1) but not zero, then selective packet drop down attack can take place.

N2 = No. of packets originated from some other nodes but received

from the neighbor node/Number of packets received

from the neighbor node Ack = Acknowledgement 0 or 1.

If the acknowledgement is received from the destination node for the data transmission, then all nodes in that path will be assigned value 1; otherwise, the assigned value is 0.

3.3 Routing Mechanism

If the source node wants to transmit a packet to the destination node, then RREP or route reply packet is sent to the neighboring node [9]. The source node selects the most trusted path [14, 15] among the available trust values of the nodes. If source node's one hop neighbor is GOOD node, then source node selects that path for the

Table 2 Path selected by node based on the proposed scheme

Next hop neighbor in the best-suited routing path (P1)	Next hop neighbor in the second best-suited path (P2)	Action taken to choose the path
G	G	G is selected in routing path P1 or routing path P2 based on length of the route available between source and destination
G	Uk	G is selected in routing path P1
Uk	G	G is selected in routing path P2
Uk	Uk	Uk is selected in routing path P1 or routing path P2 based on length of the route available between source and destination
G	B	G is selected in routing path P1
B	G	G is selected in routing path P2
B	B	B is selected in routing path P1 or routing path P2 based on the length of the path
Uk	B	Uk is selected in routing path P1
B	Uk	Uk is selected in routing path P2

where G = Good, Uk = Unknown, and B = Bad

packet transmission. If the source node's one hop neighbor is UNKNOWN or BAD node, and two hop neighbors are GOOD node, then it will choose second path, i.e., through GOOD node. Similarly, an optimal path is selected on the basis of degree of association existing between two neighboring nodes (Table 2).

3.4 Routing Algorithm

Source node broadcasts a RREQ to destination node, and source node receives RREP packet from destination node; then, we calculate the trust value of every node and action taken to identify the attack is based on the trust value (Table 3).

Table 3 Notation used in proposed algorithm

Source Node	SN
Destination Node	DN
Intermediate Node	IN
Next Hop node	NHN
Reliable node	The node through which the source node has routed packets

If (RREP is receiving GOOD node trust value) {
Route data packets value (Secure route)//that means packet is coming from secure node}
Else {
If (RREP is receiving from the UNKNOWN node trust value)
Route data packets value (Secure route)}
Else {
If (RREP is from malicious node)
Do not route data packets value (Insecure route packet)
Node may be launch a blackhole node}

4 Implementation and Results

This section explains the various performance metrics that are required for the evaluation of the network [7]. To reiterate the blackhole attack within the vehicular ad hoc network, we will begin with the explanation of performance metrics that include distribution of nodes in VANET [16], energy of nodes in network in the presence of malicious node, comparison of latency in the presence of malicious node, performance of normal node in the presence of malicious node [17, 18], data transmission rate between source and destination in the presence of malicious node [19, 20], no. of data packets transmitted from source node, and no. of data packets received by destination node.

As it is already mentioned previously that when packets are to be transmitted before source and destination, it is important that destination node should lie between the transmission regions of the source node. Here, in Fig. 4, transmission of data takes

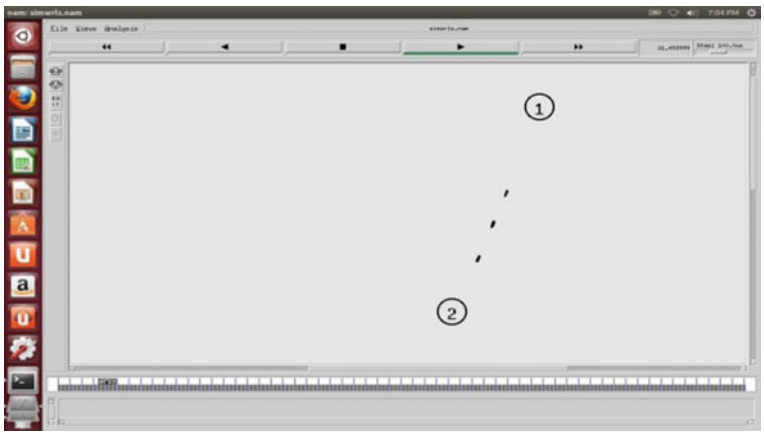

Fig. 4 Packet transmission between node 1 and node 2

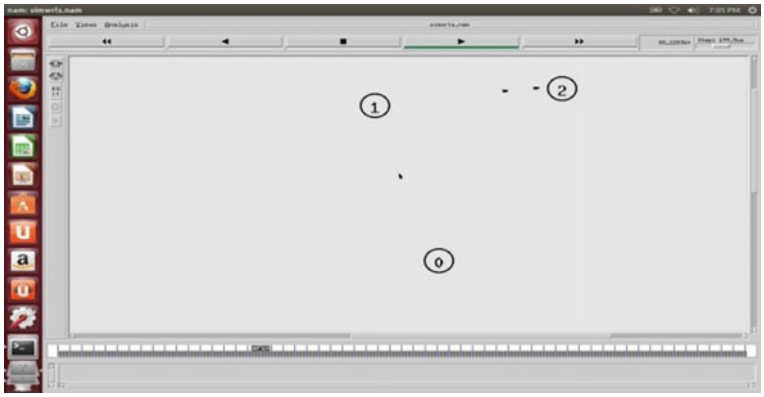

Fig. 5 Packet transmission from node 0 to node 2 via node 1

place between node 1 and node 2, and both the nodes lies between the transmission ranges of each other.

In Fig. 5, the two nodes, the node 0 and 2, do not lie within the transmission range of one another; therefore, transmission of data between node 0 and node 2 takes place through node 1 which lies within the transmission range of both the nodes.

4.1 Rebroadcasting Request Message to the Neighboring Nodes

As already discussed, we have used AODV protocol in vehicular ad hoc network [8]. The property of the AODV protocol [21] is that before sending packets to the destination, source node broadcasts a message within the network [22]. This is depicted below:

In Fig. 6, node 1 broadcasts a request message to its neighboring nodes [23]. Here, those nodes which will receive the request will send the reply to the source node which is node 1 (Fig. 7).

The message broadcasted by node 1 is received by node 0. Node 1 acts as a source node and then started sending packets to the node 0 which is a destination node. Node 0 act as a source node and start boradcasting the packet (Fig. 8).

In the above diagram, node 0, node 1 and node 2 simultaneously broadcast request message within the network to neighboring nodes.

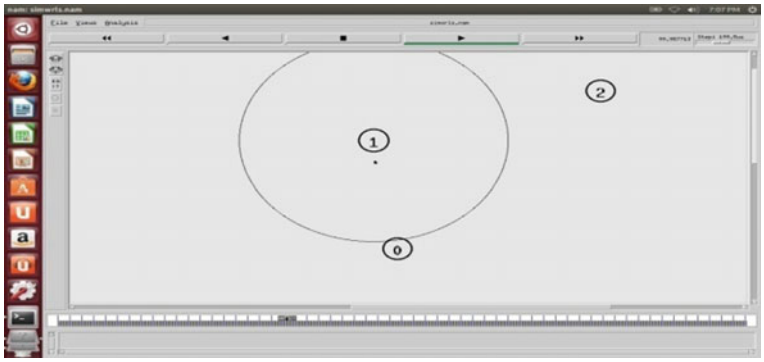

Fig. 6 Node 1 broadcasts message to its neighbors

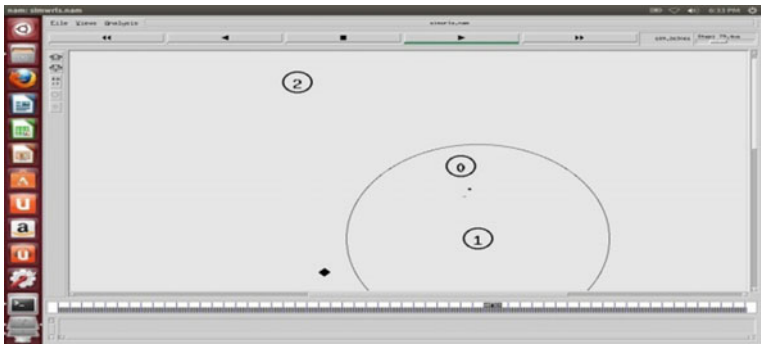

Fig. 7 Node 0 receives the message broadcasted by node 1

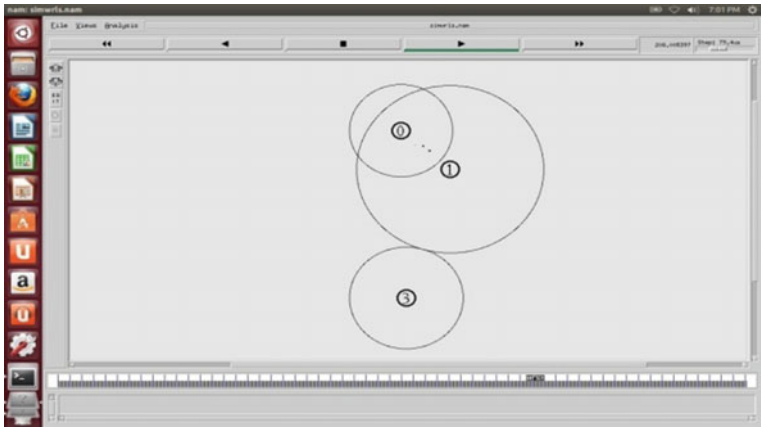

Fig. 8 Node 0, node1, and node 2 simultaneously broadcast message

4.2 *Malicious Node Drop Packets*

In Fig. 9, node 2 and node 0 act as malicious nodes [24] and while transmitting data between the source node and the destination node, they are dropping the packets.

Similarly, in Fig. 10, node 0 is acting as a malicious node and when it gets the packets from the source node (SN), then it starts dropping the packets.

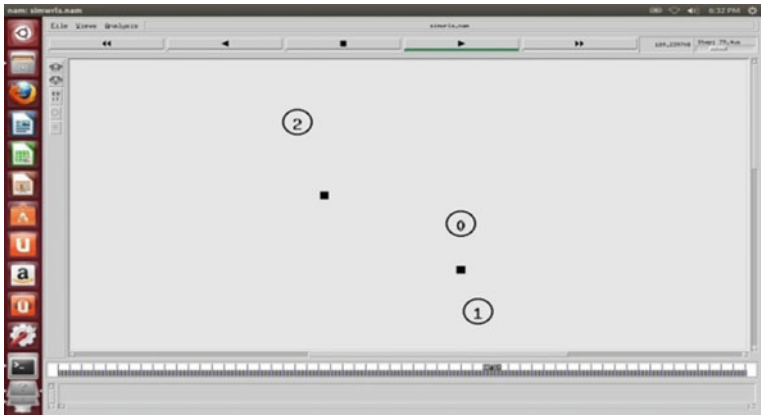

Fig. 9 Malicious node 0 and node 2 drop packets

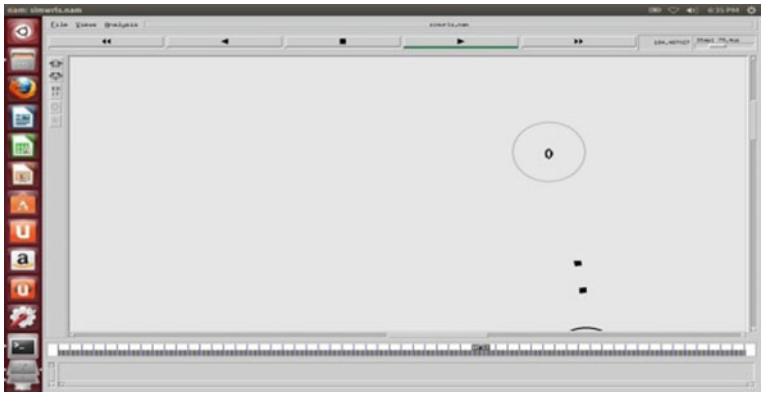

Fig. 10 Malicious node 0 drop packets

5 Conclusion

The ability to deploy a network is the characteristic of the vehicular ad hoc network. Despite of having numerous advantage and vast potential of VANET, there are some of the challenges which still remain to be overcome. One of the main problems or challenges that vehicular ad hoc network is facing is regarding the security of the network. We have analyzed various techniques and protocols that are employed in VANET. And also we have studied the behavior of security threats and challenges from which VANET suffers. Since a decade, many problems are analyzed and many solutions have been proposed to overcome those challenges. The research work was done in past mainly used to focus on designing of new protocol, comparisons between the existing protocols or making improvement in the existing protocol before standard VANETs routing protocols were defined. Though they were effective, they are not fully capable of treating those problems and are not efficient. After studying and analyzing various approaches developed till now, in my opinion the technique fits well in my scenario. This approach was regarding the exchange of messages between the nodes, the delivery of message source node, and the destination which lead to the improvement in the network performance and secure the network from blackhole attack.

References

1. Harsch, C., Festag, A., Papadimitratos, P.: Secure position-based routing for VANETs. IEEE, **2**(12) (2007)
2. Hortelano, J., Ruiz, J.C., Manzoni, P.: Evaluating the usefulness of watchdogs for intrusion detection in VANETs. IEEE Xplore **11** (2010)
3. Mathew, M.E., Arun Raj Kumar, P.: Threat analysis and defence mechanisms in VANET. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **3**(1) (2013)
4. Gonzalez-Tablas, A.I., Ribagorda, A., de Fuentes, J.M.: Overview of security issues in vehicular Ad-hoc networks. In: Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts, vol. 12(10) (2011)
5. Singh, A.P., Kateshiya, J.K.: Review to detect and isolate malicious vehicle in VANET. Int. J. Innov. Res. Sci., Eng. Technol. **4**(2) (2015)
6. Cavalli, A., LA, V.H.: Security attacks and solutions in vehicular Ad-hoc networks: a survey. Int. J. Ad-Hoc Netw. Syst. (IJANS) **4**(2) (2014)
7. Joshi, N., Dixit, K., Joshi, K.K.: A novel approach of trust based routing to select trusted location in AODV based VANET: a survey. Int. J. Hybrid Inf. Technol. **8**(7) (2015)
8. Mittal, M.: Prevention of gray hole attack in mobile Ad-Hoc Networks by enhanced multipath approach. Int. J. Adv. Res. Comput. Eng. Technol. (IJARCET) **4**(5) (2015)
9. Biswas, S., Misic, J., Misic. V.: DDoS Attack on WAVE enabled VANET through synchronization. In: IEEE Global Communications Conference (GLOBECOM '12) (2012)
10. Agrawal, A., Garg, A., Chaudhiri, N., Gupta, S., Devesh, P., Roy, T.: Security on vehicular ad hoc networks (VANET): a review paper. Int. J. Emerg. Technol. Adv. Eng. **3**(1) (2013)
11. Zeadally, S., Hunt, R., Chen, Y.S., Irwin, A., Hassan, A.: Vehicular ad hoc networks (VANETS): status, results, and challenges. Springer **50**(4) (2012)
12. Gajbhiye, T., Waoo, A.A., Pathija, P.S.: Traffic Management through inter-communication between cars using VANET system. Int. J. Adv. Comput. Eng. Commun. Technol. **1**(1) (2007)

13. Avinash, P., Jadhao, Chaudhari, D.N.: Security aware Adhoc on demand distance vector routing protocol in vehicular Adhoc network. Int. J. Eng. Appl. Technol. **2**(12), (2015)
14. Aaseri, R., Roberts, N., Choudhary, P.: Trust value algorithm: a secure approach against packet drop attack in wireless ad-hoc networks. Int. J. Netw. Secur. Appl. (IJNSA) **5**(3) (2013)
15. ViswaJhananie, K.R., Chandrasekar, C.: Detection and removal of blackhole attack using handshake mechanism in MANET and VANET". IOSR J. Mob. Comput. Appl. (IOSR-JMCA), **2**(1) (2015)
16. Yadav, R., Hemrajani, N., Goyal, D., Shivani, S.: Vulnerabilities, attacks and their detection techniques in ad hoc network. Int. J. Comput. Appl. **2**(11) (2011)
17. Gurpreet, S.S.: Malicious data detection in VANET. Int. J. Adv. Res. Comput. Commun. Eng. **1**(7) (2012)
18. Abumansoor, O., Boukerche, A.: Towards a secure trust model for vehicular ad hoc networks services. IEEE Xplore **5**(9) (2011)
19. Bhatia, J., Shah, B.: Review on various security threats & solutions and network coding based security approach for VANET. Int. J. Adv. Eng. Technol. **2**(11) (2013)
20. Mustary, N.R., Chander, R.P., Ahmed Baig, M.N.: A performance evaluation of VANET for intelligent transportation system. World J. Sci. Technol. **2**(10) (2013)
21. Prajapati, N.K., Grover, J., Gaur, M.S.: Implementation of temporal attacks in vehicular ad hoc networks. Int. J. Comput. Appl. **12**(5) (2011)
22. Dadheech, D., Goyal, D., Srivastava, S., Choudhary, C.M.: An efficient approach for big data processing using spatial Boolean queries, J. Stat. Manag. Syst. (JSMS), Taylor & Fr. Group J. ISSN:0972-0510 (Print), ISSN 2169-0014 (Online), **21**(4), 583–591 (2018). https://doi.org/10.1080/09720510.2018.1471258
23. Lipiński, B., Mazurczyk, W., Szczypiorski, K., Śmietanka, P.: Towards effective security framework for vehicular Ad-Hoc networks. J. Adv. Comput. Netw. **3**(2) (2015)
24. Kumar, A., Sinha, M.: Overview on vehicular ad hoc network and its security issues. In: 2014 International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, pp. 792–797. https://doi.org/10.1109/indiacom.2014.6828071

Anil Chaudhary · Chothmal Choudhary ·
Mukesh Kumar Gupta · Chhagan Lal ·
Tapas Badal *Editors*

Microservices in Big Data Analytics

Second International, ICETCE 2019, Rajasthan, India, February 1st-2nd 2019, Revised Selected Papers

Springer