EasyChair Preprint

№ 2550

Blackhole Attack Mitigation in Vehicular Networks: A Survey

Haris Mashood, Muazzam A. Khan and Balawal Shabir

February 5, 2020

Blackhole Attack Mitigation in Vehicular Networks: A Survey

[1]Haris Mashood, [2]Muazzam A. Khan, [1]Balawal Shabir
[1]*Department of Computing, School of Electrical Engineering and Computer Science (SEECS), National University of Sciences and Technology (NUST),* Islamabad, Pakistan.
[2]Department of Computer Science, Quaid-i-Azam University, Islamabad, Pakistan.
hmashood.mscs18seecs@seecs.edu.pk, muazzam.khattak@seecs.edu.pk, bilawalshabir@gmail.com

Abstract*— *Vehicular Ad-Hoc Networks (VANETs) are a highly dynamic Mobile Ad-Hoc Network (MANNET), which can provide proficient and safe conveyance among vehicles and road side units or base stations. The vehicles in VANET are intelligent as they are able to communicate with their surrounding neighbors; referred as nodes. Vehicular Ad hoc Networks are gaining interest of researchers worldwide because in future they will modernize driving experience by providing things from localized traffic updates, sudden car braking, adaptive cruise control and many other things. However, security concerns generally seen in ad-hoc networks or unique to VANET, present great challenges in terms of integrity, client validation, anonymity and privacy. In this paper we will go through different security threats to VANETs, how those attacks can disrupt the VANETs and different possible solutions for those attacks.

Keywords*— *VANET security, Smart Vehicles, Cryptography, Black-hole attack, IDS, ECDLP

I. Introduction

Vehicular Ad Hoc Networks makes the most of new technologies by including newer generations of wireless networks with vehicles, communication between nodes and RSUs is done by creating a robust Ad-Hoc network between mobile nodes and the RSUs. Since it is based on MANETs, it forms communication between nearby vehicles/nodes (V2V) and neighboring fixed apparatus (V2I) [1], generally known as roadside apparatus or road side units (RSU) [2]. VANET can attain affective communication between nodes by using different ad-hoc networking tools such as IRA, Wi-Fi, WiMAX, Bluetooth [3].

VANETs are mostly used for providing real time information regarding safety and traffic management which directly affect lives of people [4]. Safety is recognized as the main characteristic of VANET; hence the need for simplicity and security is of the utmost importance for these types of networks. Nearly the entirety of the nodes in the Vehicular Ad Hoc Network can form networks of their own with having any previous knowledge of the other surrounding nodes hence this feature makes VANET's have application ranging from but not limited to commercial and consumer usage with added security to ensure safety in the network. VANET with low security level are more susceptible to frequent attacks [4].

Figure 1 shows how a black-hole attack occurs when node A tries to transmit packets to node E and node G, whereas car H acts as malicious node, by advertising

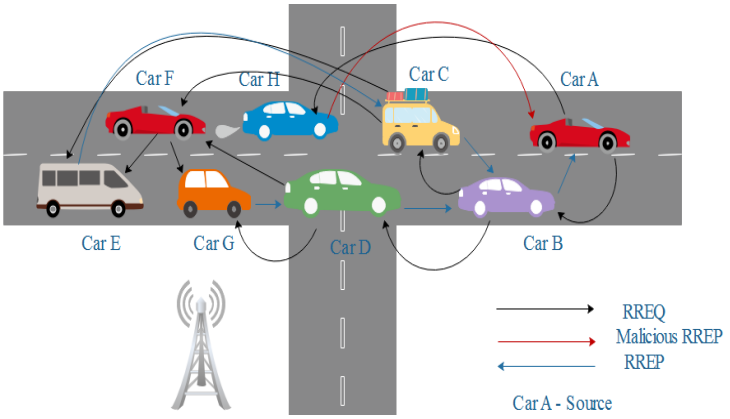

Figure 1: Black-hole Attack

false route replies against route request of car A. Routing attacks are the types of attacks in routing protocols belonging to the network layer are exploited, this is type done by dropping the packet or by disturbing the routing process of the network. The most common Routing attacks are: Grey-hole, Wormhole and Black-hole attacks [5][2].

In above mentioned black-hole attack, the attacker invites other nodes to transfer packets through the malicious node. This is achieved by sending the Malicious Route Reply (MRR) with new route details and very low hop count value [6]. A Route Request also known as RREQ is broadcasted to all of the nearby nodes and those nodes forward that Route Request to their neighboring nodes until a route to the destination is found, the malicious node replies with a false path suggesting that it has the shortest route to the destination. After the reply source node is attracted to the malicious node and sends every packet to the attacker node which the node silently drops. This effect is known as a black-hole attack. A black-hole can either be created by only a single node or with the help of

multiple nodes with the malicious intent to drop packets of other nodes [7][8][9][10].

Section II of this paper deals with literature review carried out for the purpose of dealing with the black-hole attack, several techniques are defined in this section. Section III provides comparison between techniques discussed in section II, the comparative analysis is carried out using a number of different parameters. Section IV concludes the paper and provides some insight into what can be done to improve these techniques in the future.

II. Literature Review

Ad hoc network is formed when multiple nodes that are mobile in nature connect with each other using route messages to create a network without a backbone infrastructure like routers or an administrative policy [11], VANET consists of nodes have high mobility and hence are not bounded by the structure of the network, these nodes tend to securely communicate information which is time sensitive in nature which is then disrupted by the malicious nodes under the black-hole attack which drops messages by providing false routes [12], the approaches mentioned in this section of literature review provide different methods to tackle the black-hole attack.

2.1 Certificate-less

Certificate-less cryptography is used in techniques which fall under the certificate-less category. This is done to avoid the problems caused by key escrowing, certificate-less cryptography is a variant of ID-based cryptography. In this cryptography technique the process of key generation is divided between the Key Generation Center (KGC) and the user. This increases data integrity and ensures more secure communication [13].

2.1.1 Certificate-less Conditional Privacy-Preserving Authentication scheme (CCPPA)

The approach presented by the author is used for Vehicle to Interface (V2I) communication in VANETs. CCPPA is based on Elliptic Curve Cryptography and certificate-less cryptography, CCPPA comprises of 4 stages which are: initialization, which is the start of the system; partial private key mining (extraction) and pseudo identity generation which is a process that takes place between the nodes and TA (TRA, KGC); message signing and private key generation, is the stage where the node creates the private key, signs it and the broadcasts it to the RSU containing the pseudo identity, traffic related messages and signature and timestamps; and message verification. The approach offered here was not only secure in the random oracle model under the Elliptic Curve Discrete Logarithm (ECDLP) assumption but was also successful in satisfying requirements regarding security from message authentication to preserving conditional privacy. Moreover, this approach need no bilinear pairing procedures and operations based on map-to-point hash [14].

2.1.2 Secure Certificate-less Authentication and Road Message Dissemination Protocol (SCARMDP)

A method name secure certificate-less authentication and road message dissemination protocol (SCARMDP) is suggested by the authors which is designed with the purpose to enhance the transmission security and ensuring the delivery of encrypted (road) messages to matching road side unit, the security is enhanced using bilinear pairing which is based on elliptic curve, with this in use vehicles which are within the operative range can be recognized and are given a group key [15].

2.1.3 Practical Certificate-less Conditional Privacy Preserving Authentication (PCPA)

The authors proposed an approach known as PCPA which works similarly like CCPPA but it differs from it with the use of CLS-MR which under the assumption of ECDL can be proven secure in a random oracle model, it a method having certificate-less signature with message recovery. PCPA also have the 4 stages like CCPPA which are initialization of the system, generation of pseudo identity and partial private key mining (extraction), public/private key creation along with message signing and lastly authentication of messages stage. PCPA needs no operations based on map-to-point hash functions and bilinear operations, hence making it more efficient in communication and computational cost [16].

2.2 Cryptographic Based

In Cryptographic approaches, certain cryptographic techniques are employed to protect the communication amid the nodes and to secure the messages being transmitted between the nodes in form of replies and requests.

2.2.1 3-D Markov Model

The authors have presented an approach known as 3-D Markov model, the key notion is that the nodes are allowed to adaptively switch between key changes and transmission back-off which are based on the information provided in the feedback, the keys used here are generated by AES and Elliptic Curve Cryptography which is crucial in eliminating the

security overhead cause by handshaking and piggybacking information. The model portrays interactions between key mismatch problems and packet collisions in different protocols using asymmetric or symmetric keys [17].

2.2.2 Authenticated Routing protocol for ad hoc Networks (ARAN)

Sanzgiri et al. introduced ARAN which uses cryptographic certificates for routing security purposes[11]. The approach also uses a process initial certification which is then trailed by a path instantiation request which promises end-to-end authentication for the communication processes. In ARAN the route is discovered by using a broadcast of route discovery by the source node which is then responded by the destination nodes using unicast routing, from source to destination these messages are authenticated at every hop and also on the reserve path. This method is as good as AODV but the main drawback of it is that the packet size is quite large which results in high overhead.

2.3 Location Based

In this approach the location of the node is taken into account which is then further used to counter the black-hole attack by employing different techniques.

2.3.1 Observing Physical Patterns (OPP)

According to the authors the ever increasing security requirements like small verification time, low computational load and less dependence on temper proof hardware is pushing towards purer digital signature based approach which are becoming more and more complex. Security and privacy preserving both should be attained at the same time bringing to light the major tradeoffs between security and privacy. The authors also suggested that we could focus on other revocation schemes instead of putting efforts in reducing the refreshing cost of CRL, this would free the vehicles of maintain the burden of carrying a huge CRL for verification of revoked vehicles, they also suggest that efforts should be made in order to verify nodes which could turn malicious in the near future by focusing on how they move in the network this would minimize the chance of attack by such nodes if they are identified beforehand [18].

2.3.2 Neighbor Based Approach (NBA)

The authors proposed a detection scheme which can be mostly used identify the black-hole attack and can also be used to find the most accurate path, the malicious nodes are identified by sending *modify_route_control* packets to get the correct route to the destination thus avoiding the malicious nodes [5].

2.4 Node Based

In node based approaches most of the control is given to the nodes, the nodes have computational power which they use to counter the black-hole attacks.

2.4.1 Ignore First Route Reply (IF-RREP)

The authors proposed a quite simple approach to tackle the effects of black-hole attacks, the approach suggests that the very first RREP after the broadcast of the RREQ should be ignored as it could potentially be from a malicious node, this approach was not so effective as the malicious node could also send a second RREP as well [19].

2.4.2 Multi Hop Path Verification (MHVP)

The authors presented the approach in which the source node is given computational capabilities which it can use to find number of possible paths to its intended destination, additionally the source node could also check the authenticity of the RREP sent by a node hence it could sort out the malicious node all by itself this in return causes delays as the node determines the authenticity of the nodes which could range from a few microseconds to delays of larger magnitude as well [20].

2.4.3 Security-Aware Ad hoc Routing (SAR)

The authors proposed the approach known as SAR which used relationships between the nodes and had some trust based values between the nodes, the results obtained using SAR had varying percentage of messages transmitted by the compromised node which indicate flaws in ad-hoc networks' communication with regard to security aspects [21].

2.5 Hybrid Approach

A hybrid approach combines both the functionalities of a location based and a node based approach. In this kind of technique certain node with computational capabilities are deployed in the network which tackle the malicious nodes.

2.5.1 Intrusion Detection System (IDS)

The approach proposed here uses IDS, IDS nodes are positioned in the network in different locations which all perform Anti-Blackhole Mechanism (ABM) estimating the malicious value of each node by measuring the abnormal difference between the RREP and RREQ of a node in the network, if the value reaches a certain threshold then the node is isolated by notifying all of the nodes in the network by the IDS which has detected the malicious node [22].

2.5.2 - A Hybrid Trust Based Intrusion Detection System (HTB-IDS)

The Hybrid Trust Based Intrusion Detection System approach was proposed by the authors which enabled the nodes present at different locations in the network to maintain and update tables, the network here is divided into three parts, all of the communication is handled by the base station here, control packets are exchanged among the base stations and sensors listen to these, the control packets contain IDs of different nodes present in the network, if the ID is not present in the packet than an increment is done in table contain at the sensors' end and once a malicious node is identified than the base station is notified through a different channel [23][9].

2.6 On-Demand Approach

In this approach the route is created whenever they are required by the source node, hence the name On-Demand. The source initiates the route discovery and this process is completed when one or all possible route to the destination are discovered and all false/improper routes are discarded [24].

2.6.1 Enhanced Ad hoc On-Demand Distance Vector (E-AODV)

The approach proposed by the authors is called E-ADOV which is an enhanced version of ADOV protocol, in this the source uses extra information known as pseudo replies packets (PRREP), information regarding all incoming packets are stored in a table, any abnormal behavior in the table is considered from the PRREP which is received from the malicious nodes and is rejected, the table is updated every so often with the PRREPs from all other nodes. The proposed approach is better than AODV, B-AODV and DSR in regards of call drop, throughput and collision rate. In dynamic network scenario E-AODV adapts faster with help of different control messages [10].

2.6.2 A Secure On-Demand Routing Protocol for Ad Hoc Networks (Ariadne)

The authors proposed an approach known as ARIADNE which is based on Dynamic Source Routing (DSR) and uses Timed Efficient Stream Loss-tolerant Authentication (TESLA) for authentication of messages, the general rule of thumb here is that the source node only trusts the destination node as all of the communication can take place using the destination node as well this is done in order to avoid blackmailing of the nodes but the destination can also blackmail other corresponding nodes connected with it hence the source maintains a separate blacklist for each node. New information is authenticated at every hop in REQUEST with the use of TESLA with ARIDANE for route discovery, until the TESLA keys are not released by the intermediate nodes the target does not send a reply. A high optimized DSR outperforms ARIADNE which has trust value between the nodes of its network [29].

2.6.3 Black-hole Prevention Using Trust Management and Fuzzy Logic Analyzer (BHP-TM&FL)

The proposed approach here uses trust based tables which are situated at every node, these tables contain trust values for nodes which are located at the distance of a single hop and for this the node keeps an eye on the amount of packets that are sent/dropped by each node. After a certain period these table are sent to the network operation center where certain fuzzy logics are used to refine the nodes based on these trust values and once it is done the new tables are forwarded to nodes except those having trust values less than a certain threshold, these nodes are malicious node and hence they are removed from the network [8].

2.7 Table-Driven Approach

This type of approach grants the nodes to maintain a single or multiple routing table(s) at their end, whenever a change occurs than each node broadcasts messages to all other nodes causing a change in topology, this approach has the benefit of providing fresh topological view to every node on any or certain even but this in return uses significant amounts of bandwidth as well [25].

2.7.1 Secure Efficient Distance Vector Routing for Mobile Wireless Ad-hoc Networks (SEAD)

The approach Secure Efficient Ad hoc Distance Vector Routing Protocol (SEAD) is based on DSDV and hash chain sequences, it prevents routing loops using destination sequence numbers to provide replay protection to the routed updated messages, SEAD protects against attacks by countering delays and by using the *best* route from the update of that sequence number. SEAD is outperforms DSDV in metrics like packet delivery but the major drawback is that overhead is increased because of the ever increasing routing paths being advertised in the network [26].

2.7.2 Honeypot based proactive Intrusion Detection System (HPBP-IDS)

According to the authors the honeypot based IDS approach uses bait to lure in the malicious nodes, this is

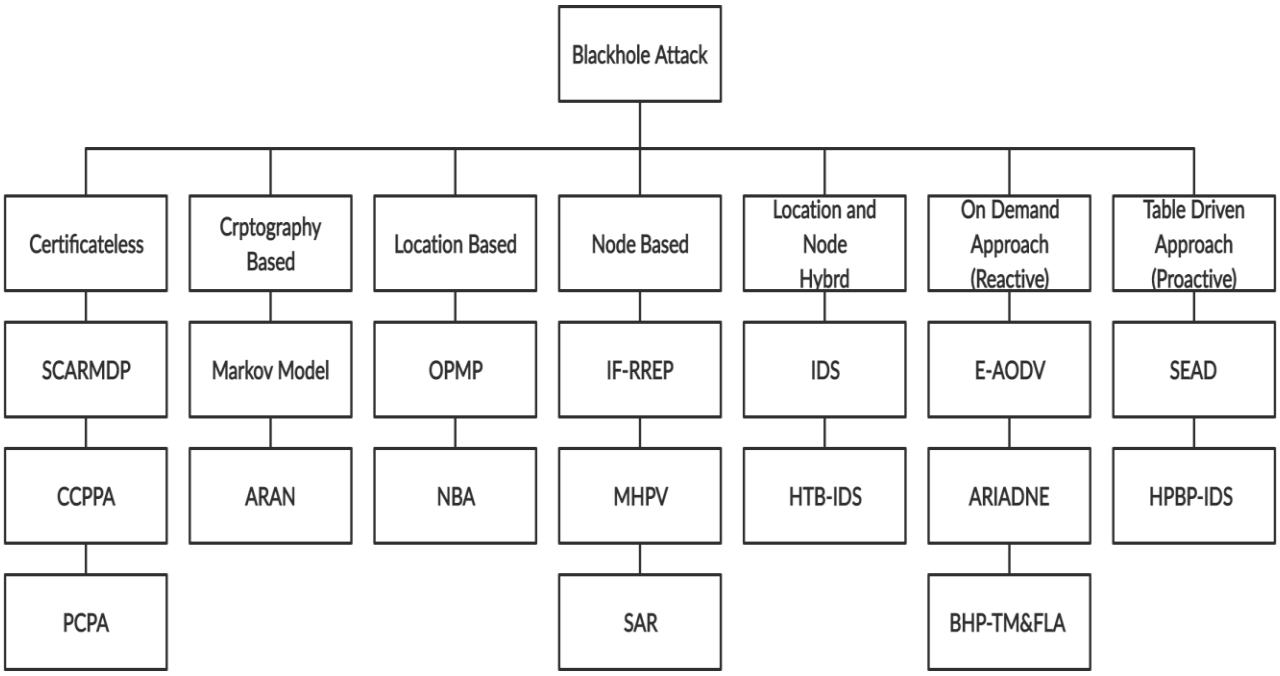

Figure 2: Taxonomy for Black-hole Prevention Schemes

done by maintaining a list of nodes which have dropped packets in the past, once a node drops a packet it is added into that suspicion selfish node list then a packet is used as a bait for confirmation, if the node drops the packet then all the paths to and from that node along with the node are deleted. This approach improves packet delivery and end-to-end delay but the major drawback of this is that it increases overhead in the network with its fake bait messages to detect malicious nodes.

III. Comparative Analysis

Following the literature review and analyzing different approaches for tackling black-hole attacks we have drawn up a comparative analysis of the different techniques used for this issue. The comparative analysis is based on different parameter which is the cost of data transmissions in terms of memory (Overhead); the ability of the approach to tackle the attack in the network (Black-hole Attack); the ability of the approach to tackle multiple malicious nodes in the network which are attacking the network simultaneously (Corporate Black-hole Attack); the rate of packets colliding in the when being simultaneously sent by different nodes (Collision Rate); the ratio with which the packets are delivered to the destination node (Packet Delivery Ratio); the rate at which the information is being sent over the network the sudden termination of the connection between nodes (Call Drop); the taken by the packet to reach the destination node from the source node (End-to-End Delay); the accuracy and correctness of the data which is received at the destination (Data Integrity) and lastly the complexity of implementation of the proposed approach (Complexity).

The techniques used in the comparative analysis are CCPPA; the Markov Approach; the observing of motion patterns; the Ignorance of First Route Reply; the Multi Hop Path Verification method; SEAD; the Honeypot Based Proactive Intrusion Detection System; ARAN; SAR; the Node Based Approach; the Intrusion Detection System (IDS); the Hybrid Trust Based IDS; SCARMDP; the Practical Certificate-less Conditional Privacy Preserving Authentication; the Enhanced AODV; ARIADNE and lastly the black-hole Prevention method Using Trust Management and Fuzzy Logic Analyzer. These techniques were compared on the previously mentioned metrics upon which the comparative analysis is based on, all of the techniques tackled the black-hole attacks but a few could tackle the corporate black-hole attack and in terms of complexity the technique which performed better was indeed more complex than its competitors and had more overhead on the network.

Techniques/Protocols	Overhead	Blackhole Attack	Corporative Blackhole	Collision Rate	PDR	Throughput	Call Drop	End-to-End Delay	Data Integrity	Complexity
CCPPA [14]	H	Y	-	H	H	H	N	H	Y	Y
Markov Approach [17]	H	Y	-	H	H	-	N	H	Y	Y
OPMP [18]	H	Y	Y	L	M	-	N	M	-	Y
IF-RREP [19]	-	Y	Y	H	H	H	N	H	Y	-
MHPV [20]	L	Y	N	L	H	H	N	H	Y	N
SEAD [26]	L	Y	-	H	H	H	N	H	Y	N
HPBP-IDS [9][23]	H	Y	-	L	H	H	N	H	Y	Y
ARAN [11]	H	Y	N	H	M	H	N	H	Y	Y
SAR [21]	H	Y	-	-	M	L	N	H	Y	Y
NBA [5]	L	Y	-	L	M	H	-	-	Y	N
IDS [22]	L	Y	Y	L	H	H	N	M	Y	Y
HTB-IDS	H	Y	-	L	H	L	N	H	Y	Y
SCARMDP [15]	-	Y	-	L	H	H	N	H	Y	Y
PCPA [16]	L	Y	-	L	H	H	N	H	Y	N
E-AODV [10]	L	Y	Y	L	M	H	N	H	Y	N
ARIADNE [27]	-	Y	-	-	H	-	N	H	Y	-
BHP-TM&FLA [8]	H	Y	N	L	H	H	N	H	Y	Y

Table 1: Comparative Analysis of Prevention Techniques

Acronym	Full Form
H	High
L	Low
M	Medium
Y	Yes
N	No
PDR	Packet Delivery Ratio
CCPA	Certificateless Conditional Privacy preserving Authentication
OPMP	Observing Physical Motion Patterns
IF-RREP	Ignore First Route Reply
MHPV	Multi Hop Path Verification
SEAD	Secure efficient distance vector routing for mobile wireless ad hoc networks
ARAN	Authenticated Routing protocol for ad hoc Networks
SAR	Security-Aware Ad hoc Routing
NBA	Node Based Approach
IDS	Intrusion Detection System
HTB-IDS	A Hybrid Trust Based IDS
SCARMDP	Secure Certificateless Authentication and Road Message Dissemination Protocol
PCPA	Practical Certificateless Conditional Privacy Preserving Authentication
E-AODV	Enhanced Ad hoc On-Demand Distance Vector
ARIADNE	A Secure On-Demand Routing Protocol for Ad Hoc Networks
BHP-TM&FLA	Black-hole Prevention Using Trust Management and Fuzzy Logic Analyzer
HPBP-IDS	Honeypot Based Proactive Intrusion Detection System

Table 2: Used Acronyms

IV. Conclusion and Future Work

In this paper we have discussed what a black-hole attack is and what are the effects of black-hole attack along with different black-hole prevention techniques for VANETs..? Normally used cryptographic methods are not suitable for prevention of such attacks as they do not provide enhanced security hence these black-hole attacks can cause disruptions and congestions in the network. We have discussed multiple novel approaches which can be used to tackle this problem. Techniques like SEAD, IDS and CCPPA are good but more work need to be done in order to develop new and more

efficient schemes. Present schemes can also be improved as well. Also from the results of comparative analysis we suggest that by adopting different preventive solution suggested above the effects of black-hole attack can be reduced drastically, also worth mentioning here is that we all vehicle are VANET enabled and are also homogenous in nature.

References

[1] C. Shao, S. Leng, Y. Zhang, A. Vinel, and M. Jonsson, "Analysis of connectivity probability in platoon-based Vehicular Ad Hoc Networks," in *IWCMC 2014 - 10th International Wireless Communications and Mobile Computing Conference*, 2014, pp. 706–711.

[2] N. K. Chaubey, "Security analysis of vehicular Ad hoc networks (VANETs): A comprehensive study," *Int. J. Secur. its Appl.*, vol. 10, no. 5, pp. 261–274, 2016.

[3] A. S. K. Pathan, "*Security of Self-Organizing Networks MANET," WSN, WMN, VANET*. 2011.

[4] D. Chadha, "Vehicular Ad hoc Network (VANETs): A Review," 2015.

[5] N. Nandini and R. Aggarwal, "Prevention of blackhole attack by different methods in MANET," *Network*, vol. 4, no. 2, pp. 297–300, 2015.

[6] P. N. Raj and P. B. Swadas, "DPRAODV: A Dynamic Learning System Against Blackhole Attack In AODV Based MANET," *Int. J. Comput. Sci. Issues*, vol. 2, no. 1, pp. 54–59, 2009.

[7] P. A. N. Upadhyaya, "Blackhole Attack Prevention in VANET," *Int. J. Futur. Revolut. Comput. Sci. Commun. Eng.*, vol. 3, no. October, pp. 222–229, 2017.

[8] N. Rafique, M. A. Khan, N. A. Saqib, F. Bashir, C. Beard, and Z. Li, "Blackhole Prevention in VANETs Using Trust Management and Fuzzy Logic Analyzer," *Int. J. Comput. Sci. Inf. Secur.*, vol. 14, no. 9, p. 1226, 2016.

[9] S. Ali, M. A. Khan, J. Ahmad, A. W. Malik, and A. Ur Rehman, "Detection and prevention of Blackhole Attacks in IOT & WSN," *2018 3rd Int. Conf. Fog Mob. Edge Comput. FMEC 2018*, pp. 217–226, 2018.

[10] P. Tyagi and D. Dembla, "Performance analysis and implementation of proposed mechanism for detection and prevention of security attacks in routing protocols of vehicular ad-hoc network (VANET)," *Egypt. Informatics J.*, vol. 18, no. 2, pp. 133–139, 2017.

[11] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A secure routing protocol for ad hoc networks," in *10th IEEE International Conference on Network Protocols, 2002. Proceedings.*, 2005, pp. 78–87.

[12] A. Upadhyaya, "Blackhole Attack and its effect on VANET International Journal of Computer Sciences and Engineering Open Access Blackhole Attack and its effect on VANET," no. November 2017, 2018.

[13] "Certificateless cryptography - Wikipedia." [Online]. Available: https://en.wikipedia.org/wiki/Certificateless_cryptography. [Accessed: 29-Nov-2019].

[14] Y. Ming and H. Cheng, "Efficient certificateless conditional privacy-preserving authentication scheme in VANETs," *Mob. Inf. Syst.*, vol. 2019, 2019.

[15] H. Tan, D. Choi, P. Kim, S. Pan, and I. Chung, "Secure Certificateless Authentication and Road Message Dissemination Protocol in VANETs," *Wirel. Commun. Mob. Comput.*, vol. 2018, 2018.

[16] Y. Ming and X. Shen, "PCPA: A practical certificateless conditional privacy preserving authentication scheme for vehicular Ad Hoc networks," *Sensors (Switzerland)*, vol. 18, no. 5, pp. 1–23, 2018.

[17] X. Zha *et al.*, "Analytic model on data security in VANETs," *2017 17th Int. Symp. Commun. Inf. Technol. Isc. 2017*, vol. 2018-Janua, pp. 1–6, 2018.

[18] F. Qu, Z. Wu, F. Wang, and W. Cho, "A Security and Privacy Review of VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 2985–2996, 2015.

[19] S. Dokurer, Y. M. Erten, and C. E. Acar, "Performance analysis of ad-hoc networks under blackhole attacks," *Conf. Proc. - IEEE SOUTHEASTCON*, pp. 148–153, 2007.

[20] M. Al-Shurman, S. M. Yoo, and S. Park, "Blackhole attack in mobile ad hoc networks," *Proc. Annu. Southeast Conf.*, pp. 96–97, 2004.

[21] S. Yi, P. Naldurg, and R. Kravets, "Security-aware ad hoc routing for wireless networks," *Proc. 2001 ACM Int. Symp. Mob. Ad Hoc Netw. Comput. MobiHoc 2001*, pp. 299–302, 2001.

[22] M. Y. Su, "Prevention of selective blackhole attacks on mobile ad hoc networks through intrusion detection systems," *Comput. Commun.*, vol. 34, no. 1, pp. 107–117, 2011.

[23] M. M. Ozcelik, E. Irmak, and S. Ozdemir, "A hybrid trust based intrusion detection system for wireless sensor networks," *2017 Int. Symp. Networks, Comput. Commun. ISNCC 2017*, pp. 1–6, 2017.

[24] S. Kalwar, "Introduction to reactive protocol," *IEEE Potentials*, vol. 29, no. 2, pp. 34–35, 2010.

[25] "List of ad hoc routing protocols - Wikipedia." [Online]. Available: https://en.wikipedia.org/wiki/List_of_ad_hoc_routing_protocols. [Accessed: 29-Nov-2019].

[26] Y. C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," *Proc. - 4th IEEE Work. Mob. Comput. Syst. Appl. WMCSA 2002*, vol. 1, pp. 3–13, 2002.

[27] Y.-C. HU, A. PERRIG, and D. B. JOHNSON, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," *Proc. - Int. Conf. Netw. Protoc. ICNP*, pp. 78–87, 2005.