Hindawi
Mobile Information Systems
Volume 2020, Article ID 2168086, 9 pages
https://doi.org/10.1155/2020/2168086

Research Article

Efficient Protection Mechanism Based on Self-Adaptive Decision for Communication Networks of Autonomous Vehicles

Min Zhao, Danyang Qin, Ruolin Guo, and Guangchao Xu

Key Lab of Electronic and Communication Engineering, Heilongjiang University, Harbin, China

Correspondence should be addressed to Danyang Qin; qindanyang@hlju.edu.cn

Received 9 July 2019; Revised 16 December 2019; Accepted 27 May 2020; Published 10 June 2020

Academic Editor: Massimo Condoluci

The communication network of autonomous vehicles is composed of multiple sensors working together, and its dynamic topology makes it vulnerable to common attacks such as black hole attack, gray hole attack, rushing attack, and flooding attack, which pose a threat to the safety of passengers and vehicles; most of the existing safety detection mechanisms for a vehicle can only detect attacks but cannot intelligently defend against attacks. To this end, an efficient protection mechanism based on self-adaptive decision (SD-EPM) is proposed, which is divided into the offline phase and the online phase. The online phase consists of two parts: intrusion detection and efficient response. Attack detection and defense in the vehicular ad hoc networks (VANETs) are performed in terms of the attack credibility value (AC), the network performance attenuation value (NPA), and the list of self-adaptive decision. The simulation results show that the proposed mechanism can correctly identify the attack and respond effectively to different attack types. And, the negative impact on VANETs is small.

1. Introduction

With the promotion of autonomous vehicles in life, the safety of vehicular ad hoc networks (VANETs) (explanations of all abbreviations in the text are given in the end) has become crucial. Automated driving technology not only requires a large number of sensors to collect environmental data, but also needs to send a large amount of collected data to other vehicles and data centers. These data are related to the owner's private information and the safety of the vehicle. Once damaged, it will pose a threat to the safety of people and the vehicle. Therefore, protecting VANET from internal/external attacks becomes very imperative. VANET is an adaptive wireless network that connects mobile vehicles in which mobile vehicles work together by transmitting data packets to each other. The working principle of an autonomous vehicle is shown in Figure 1. The sensors, the communication system, and the on-board units (OBU) cowork to provide a wide range of services for vehicles and the infrastructure [1]. Wherein, the OBU-enabled vehicle can transmit and receive messages with other vehicles or road side units within the radio coverage via the communication system. Autonomous vehicles require the latest motion data, communication protocols, and assistance of positioning systems to achieve efficient and reliable exchange of information with each other. The autonomous vehicle transmits a warning message and a cooperative awareness message (CAM) over the wireless network to transmit its own state to other vehicles within the radio coverage to determine the motion state of each vehicle, ensuring the normal operation of the vehicle system. The devices on autonomous vehicles play a vital role in providing short-range wireless ad hoc networks for transmitting the required motion and control data to the vehicle network, helping to improve the efficiency and safety of traffic [2]. However, the random movement of the vehicle, the stalling at any time, the speed of the vehicle, the high dynamic topology, the lack of a fixed security system, and the peak period of the road [3] will enable the intruder to launch an attack without physical access, which brings serious security problems to VANETs.

Traditional systems cannot protect the sensitive information or control data of a communication system or the host device from internal/external attacks. Therefore,

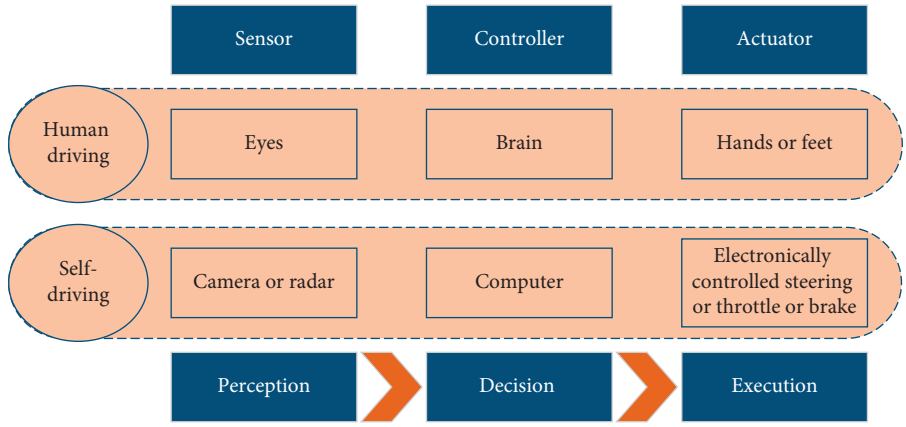

Figure 1: The principle of autonomous vehicles.

protecting VANETs from internal/external attacks is imperative for the safety of people and vehicles. An efficient protection mechanism based on self-adaptive decision for VANETs is designed, which will combine knowledge-based intrusion detection technology [4] and anomaly-based intrusion detection technology [5] and be based on a designed self-adaptive decision list to flexibly defend against common attacks in VANET environments, thereby providing technical guarantee for the security application of the future VANETs.

The rest of this paper is organized as follows: Section 2 briefly introduces some of the existing detection methods for VANETs. Section 3 describes the algorithm of the offline phase and the online phase of the SD-EPM. Section 4 gives the simulation results and analysis. Finally, Section 5 summarizes this paper.

2. Related Work

The safe work of autonomous vehicles is inseparable from the normal operation of VANET. However, the external communication system of VANET is vulnerable to various attacks, and the security issues of VANETs have attracted extensive attention.

Researchers have tried several schemes to protect VANETs. Gong et al. [6] proposed a method for applying the public key infrastructure (PKI) technology to VANETs. The method uses vehicle identification (ID) and radio frequency identification (RFID) to map the IPv6 interface and the vehicle private key in the certificate authority (CA), and then the CA calculates the vehicle's public key according to the private key and sends it to the vehicle. The vehicle communicates with the road side unit (RSU) in the public key distributed by the CA to obtain an anonymous key. Finally, the vehicle communicates with others using an anonymous key from the RSU to protect the identity and privacy of vehicles and drivers. Alheeti et al. [7] used the proportional reset score (POS) method to reduce the number of functions extracted from the trace file of VANET behavior and used for classification. Artificial neural networks (ANNs) and fuzzification data are used to detect black hole attacks. Gmiden et al. [8] proposed a simple controller area network (CAN) bus intrusion detection system (IDS). First, the CAN ID of the transmitted message is checked through an IDS, then the time interval of the latest message is calculated, and finally the time interval of the CAN message is analyzed to achieve the denial of service (DoS) detection of attacks and other types of attacks. Alheeti and Mcdonald-Maier [9] proposed the ICMetric-IDS detection system, which is based on the characteristics of the magnetometer sensor's offset value and the trace file extracted from the simulated vehicle network traffic and the integrated circuit metering technology to achieve protection for the communication system. However, most of the above detection systems can only target fixed attacks and do not consider the defense response to attacks.

Based on the above deficiencies, we will design a protection mechanism that not only correctly detects multiple attacks, but also adaptively performs different and effective responses according to the detected AC and NPA of the attacks in VANETs.

3. The Algorithm of SD-EPM

The data center of VANETs includes data management, equipment management, and operation management to achieve unified and secure network access, flexible adaptation of various terminals, and collection and analysis of massive data. The vehicle is equipped with various sensor data, various collected data, and GPS information and reports to the data center through the wireless network. The data center can obtain vehicle state information and vehicle position information in real time through calculation. If the external communication network of the autonomous vehicle is damaged, serious human and vehicle safety problems will occur. Therefore, SD-EPM is designed for external communication of autonomous vehicles. An overall architecture of the SD-EPM is shown in Figure 2, which consists of an offline phase and an online phase.

3.1. Offline Stage of SD-EPM. The offline phase of SD-EPM consists of two tasks: establishing a network matrix and performance matrix and building an initial file.

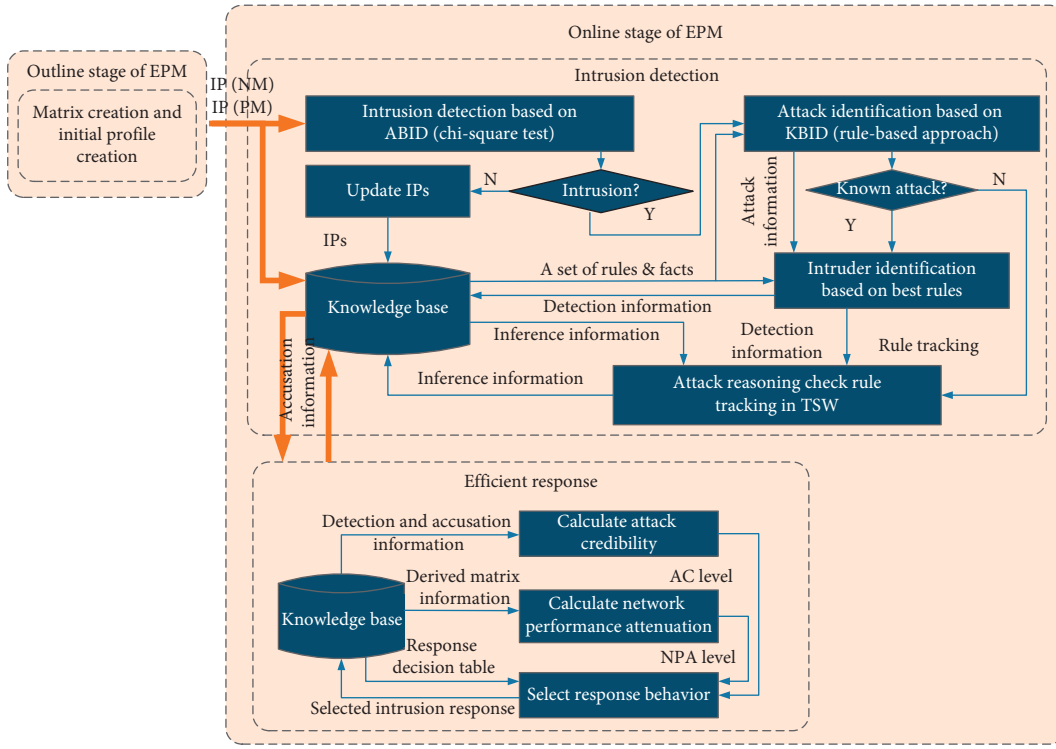

Figure 2: Overall block diagram of the SD-EPM.

3.1.1. Establishment of Key Matrix. SD-EPM periodically collects data in the external communication network of the autonomous vehicle, in order to realize real-time monitoring and protecting for VANET. The specific process means that after each time interval (T), each vehicle node (VN) transmits data to the central vehicle node (CVN) [10], and then the CVN stores the data in a network matrix (NM) and a performance matrix (PM). The CVN then reports these matrix data to the management vehicle node (MVN).

Every car in VANETs can be seen as a router or a host [11]. This paper uses AODV [12] as the basic routing algorithm to illustrate the principle of the proposed mechanism. NM consists of a matrix of $(r \times c)$, where r is the abbreviation of the row, c is the abbreviation of the column, and the number of r and c depends on the parameters of NM:

NM = {RREP (route reply), RREQ (route request), RERR (route error), TTL (time to live value), RREQ_scr_seq (route request source sequence), RREP_dest_seq (route reply destination sequence), and RREQ_dest_seq (route request destination sequence)}.

The rows represent different parameters, and the columns represent the data content contained in the parameters. The 1st row stores the RREP sequence, the 2nd row stores the RREQ sequence, the 3rd row stores the RERR sequence, the 4th row stores the TTL sequence, the 5th row stores the RREQ_scr_seq sequence, the 6th row stores the RREP_dest_seq sequence, and the 7th row stores the RREQ_dest_seq sequence. The length of each column depends on the length of the different parameter data, and each line is added as an equal-length sequence by zero padding at the end of the sequence.

The PM consists of parameters that reflect the state of the communication network, which can be drawn from the NM. Here, the PM includes 4 parameters:

PM = {RO (routing overhead), PTR (packet transmission ratio), NLP (number of lost packets), and THT (throughput)}.

The RO refers to the ratio of the number of packets received by the destination vehicle sensor to the total number of packets. PTA refers to the ratio of the number of packets received by the destination vehicle sensor to the initial number of packets of the source vehicle sensor. NLP refers to the number of lost packets during routing. THT refers to the average network throughput.

3.1.2. Establishment of Initial File. In the process of data collection, CVN continuously reports the collected NM data and PM data to the MVN in a fixed T, and then the MVN trains the collected data N times by the training model during several Ts. ${}_bX_c^a = X_1, X_2, X_3, \ldots, X_M$ are random variables representing the NM, where a represents the a-th time interval, b represents the parameter of NM, and c $(1 \le c \le M$ represents the number of ${}_bX_c^a$ in the b-th parameter of NM, where M is the maximum value of ${}_bX_c^a$ of the b-th parameter of the NM in the a-th T. Similarly, the PM is represented by ${}_bY_c^a$, and the variables have the same meaning.

The MVN calculates the probability distribution expected value $P({}_bX_c^a)$ of the NM and the probability distribution expected value $P({}_bY_c^a)$ of the PM in the time interval a. The entire process is repeated N times in each T. Then, the

MVN calculates the average values of the two matrices in the N time intervals and stores these values in the initial profile (IP) of the NM and PM. The IP reflects the driving state of the vehicle in normal VANETs.

3.2. Online Stage of SD-EPM. This section describes the architecture and algorithms of the SD-EPM. The overall block diagram of SD-EPM is shown in Figure 2. The online phase includes intrusion detection and efficient response.

3.2.1. Intrusion Detection Mechanism. The MVN uses the parameters in the NM to perform intrusion detection using a chi-square test. Chi-square test is a commonly used hypothesis testing method based on the χ^2 distribution. Its invalid hypothesis H_0 indicates that the observed value is not different from the expected value. Chi-square test is based on distance measurement and has a lower computational cost than other tests such as Hotelling T2. At this stage, the probability distribution of each parameter in the NM is first calculated, and the calculation result is stored as an observation value. Then, using the expected values above, a hypothesis test for each parameter b of the NM in T with the null hypothesis H_0 $[b]$ is performed, i.e.,

$$X^2[b] = \forall_b \left(\sum_{c=1}^{M} \left(\frac{{}_bX_c^a - \overline{{}_bX_c^a}}{\overline{{}_bX_c^a}} \right) \right), \tag{1}$$

where $X^2[b]$ is the chi-square test value and $\overline{{}_bX_c^a}$ is the observed value of the NM. Finally, the MVN performs a joint hypothesis test on all parameters of the NM. If H_0 (the observation of each parameter of the NM meets the expected value) is rejected, it is determined that an intrusion occurred in T and enters the efficient response phase. If H_0 is accepted, it is determined that no intrusion occurs in T, and the IP is updated. This paper updates the IP of the NM by the exponentially weighted moving average (EWMA):

$$\forall_b \left(\overline{{}_bX_{(q,c)}^a} = \beta \cdot X_{(q,c)}^a + (1-\beta) \cdot \overline{{}_bX_{(q,c)}^a} \right), \tag{2}$$

where $X_{(q,c)}^a$ and $\overline{{}_bX_{(q,c)}^a}$ in equation (2) represent the expected value and the observed value of the parameter b in NM when the number of update periods is q, respectively. When no intrusion is detected, the q value is increased in T. $\beta = 2/(q-1)$ is a weighting factor. Therefore, the update file reflects the current driving state of the vehicle in VANETs. The intrusion detection algorithm is shown in Algorithm 1.

3.2.2. Efficient Response Mechanism. In the efficient response mechanism, the MVN calculates the AC based on the detection information and the allegation information. Then, the NPA is calculated by the parameters in the PM. The list of self-adaptive decision is used to select an effective response behavior.

(1) Establishment of Response Behavior. A reasonable response behavior is adopted and put into the response list of efficient response, after analyzing the appropriateness of each intrusion response behavior in the possible intrusion response behavior of the VANET communication network. Then, a list of response behaviors for efficient response is proposed based on AC and NPA:

(i) Full isolation: this response behavior is selected when AC is greater than 70% and NPA is greater than 30%

(ii) Attacker bypass: when $25\% < \text{AC} \leq 70\%$ and $10\% \leq \text{NPA} \leq 30\%$, the efficient response mechanism adopts this response behavior

(iii) No punishment: when $0\% < \text{AC} \leq 25\%$ and $0 \leq \%$ NPA $< \%10$, the efficient response mechanism will simply ignore the attack

(2) Acquisition of Key Parameters. A test sliding window (TSW) is used to increase the probability of correctly detecting intrusions. The SD-EPM will only defend against intrusions when there are intrusions in the TSW of the p-dimension of multiple T. Therefore, the probability of determining an intrusion is shown in the following equation:

$$P_c = \sum_{i=d}^{p} C_i^p \cdot (P)^i \cdot (1-P)^{(p-i)}, \tag{3}$$

where p (the number of checks) is the dimension of the TSW, d is the minimum number of times for determining an intruder, $C_i^p = p!/i!\,(p-1)!$ is a binomial coefficient, P is the probability of a single detection, and P_c is the probability of confirming an intruder.

In the current TSW, the MVN performs the efficient response mechanism for all intruders identified. MVN first calculates AC by the detection information and allegation information:

$$\text{AC} = w_1 \cdot CI + w_2 \cdot P_c, \tag{4}$$

where w_i is the weighting factor, and the weight sum is 1; CI is the confidence interval for the chi-square test during the intrusion detection process.

Then, the following equation is used to calculate NPA:

$$\text{NPA} = w_1 \cdot \Delta\text{THT} + w_2 \cdot \Delta\text{PTR} + w_3 \cdot \Delta\text{RO} + w_4 \cdot \Delta\text{NLP}, \tag{5}$$

where Δ represents the percentage change between the average value of the parameter rs (throughput, packet transmission ratio, routing overhead, and number of lost packets) in the current TWS and the average when no attack occurred.

Once AC and NPA are determined, the MVN assigns a level to the AC and NPA. To this end, four AC levels are defined: $0 < \text{AC}\ (\%) \leq 25$ is "lower," $25 < \text{AC}\ (\%) \leq 50$ is "medium," $50 < \text{AC}\ (\%) \leq 70$ is "high," and $\text{AC}\ (\%) > 70$ is "very high." For the NPA level, the four levels of low, medium, high, or very high are again used.

(3) The List of Self-Adaptive Decision. The list of self-adaptive decision is shown in Table 1, where M means medium, L means low, H means high, and HV means very high.

When the VN receives the allegation packet, it first checks its broadcast address and the source address. Then, if

Do after every T
  Collect ${}_bX_c^a$ from VNs in T, $\forall_i$
  Calculate $P({}_bX_c^a)$
  Calculate averages of $P({}_bX_c^a)$ and observe as observation values
End do
For $\forall_i$ calculate CVNi-computed for ${}_bX_c^a$ by equation (1)
  Ho[b]: ${}_bX_c^a$ fits $|_bX_c^a$
  Hn[b]: ${}_bX_c^a$ does not fit $|_bX_c^a$
  If (CVNi-compute d[b] $>P$ value[b]
    Reject Ho[b]
  End if
End for
Combine null hypothesis testing
  Combine Ho: ${}_bX_c^a$ fits $|_bX_c^a$
  Combine Hn: ${}_bX_c^a$ does not fit $|_bX_c^a$
  If (combined Ho is rejected)
    Perform efficient response
  else: update IP of the NM
End if

Algorithm 1: The algorithm of intrusion detection.

Table 1: List of self-adaptive decision.

Parameter	Level and selection															
AC	M	H	HV	HV	H	L	L	H	M	M	M	L	H	HV	HV	L
NPA	HV	HV	HV	M	H	HV	H	M	H	M	L	M	L	L	H	L
Full isolation	√	√	√		√	√									√	
Attacker bypass				√			√	√	√	√						
No punishment											√	√	√	√		√

the alleged intruder V_j is already on the blacklist, the VN will ignore and remove the alleged packet. Otherwise, the intrusion response behavior specified for V_j will be checked.

If the intrusion response behavior is no punishment, the MVN will ignore the attack.

If the response behavior is full isolation, VN will add V_j into its blacklist list and then fully isolate V_j, delete all packets of V_j in the blacklist, and ignore all packets about V_j in the queue.

If the intrusion response behavior is attacker bypass, the VN will first add V_j to its temporary blacklist. Then, the existing routing packets for V_j are ignored and deleted. Also, all VNs exclude V_j from new route discoveries.

However, in order to protect the current service for data forwarding, the VN will continue to forward the data packets that have been received from V_j to the existing route until nodes find a new route around V_j. The algorithm of the efficient response mechanism is given in Algorithm 2.

4. Simulation Results and Analysis

4.1. Performance Analysis of SD-EPM. The network nodes are used to simulate real vehicles traveling in the city, and GloMoSim version 2.03 is utilized to build the simulation environment for the following simulation experiments. In the experiment, flooding attacks are formed by malicious RREQ broadcasts (i.e., denial of service attacks), black hole and gray hole attacks are formed by forged RREP packets, and rushing attacks are formed by forged RREQ packets.

4.1.1. Intrusion Detection. The performance (the success rate and false alarm rate) of intrusion detection is analyzed in different attack scenarios [13–16]. As seen in Figure 3, the average success rate of EMP in different network dimensions is 89.1%, and the average false alarm rate is 3.8% in the black and gray hole attacks, when the average speed of the vehicles is not more than 10 km/h; the average success rate of EMP in different network dimensions is 90.3%, and the average false alarm rate is 4.3% in the rushing attack, when the average speed of the vehicles is not more than 12 km/h; the average success rate of EMP in different network dimensions is 92.7%, and the average false alarm rate is 4.1% in the flooding attack, when the average speed of the vehicles is not more than 12 km/h. The proposed method shows good performance in a variety of scenarios.

In addition, it can be seen that when the average vehicle speed is greater than 43.2 km/h, the performance of the EMP will decrease because the rapid movement of the vehicle will lead to an increase in link complexity, resulting in a certain small error. However, this error does not have much impact on vehicles traveling in urban areas where speed is limited. Therefore, SD-EPM can achieve a high detection success rate and a low false alarm rate in practical applications.

For all *Ri* detected in a TSW
    Calculate AC using equation (4)
    Calculate NPA by equation (5)
    Assign AC level based on calculated AC
    Assign NPA level based on calculated NPA
    Search CVN execution table (Table 1) using AC and NPA levels and identify intrusion responding behavior (RB)
If (RB == full isolation)
    MVN adds the *Ri* into blacklists and broadcasts AP with RB = full isolation
Then If *Ri* receives packet from Rj
    If *Rj* is in blacklist list of *Ri*, ignore and delete all packets queued from *Rj*
    Else: handle and process packet
    End If
End If
Else If (RB == attacker bypass)
    MVN momently blacklists *Ri* and broadcasts AP with RB = attacker bypass
Then If *Rj* is in moment blacklist list of Ri
    If *Ri* receives data packet from *Rj*, ignore and delete RREQ, RREP, and RERR packets from *Rj*
    End If
    If *Ri* receives data packet from *Rj* destined for *Rk*.
    Ri forwards data packets to *Rk*
    End If
    Rj deletes route including *Rj* from its route table
    Else: handle and process packet
    End If
    End If
Else MVN sets RB to no punishment
    End If
End If
End If

Algorithm 2: The algorithm of the efficient response.

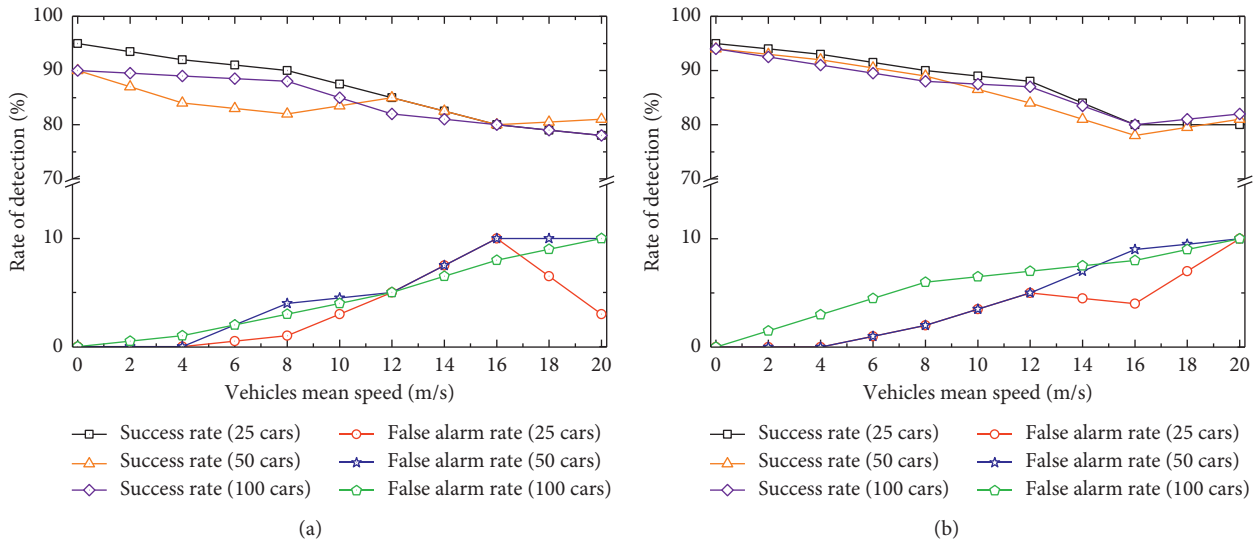

Figure 3: Continued.

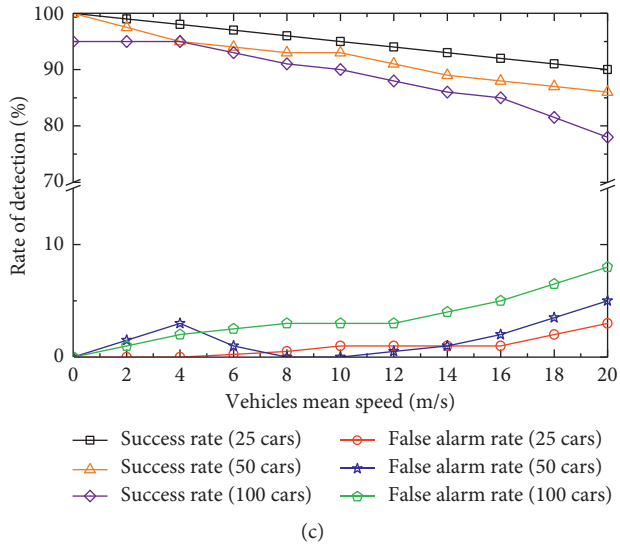

Figure 3: Success rate and false alarm rate of SD-EPM. (a) Black and gray hole attacks. (b) Rushing attack. (c) Flooding attack.

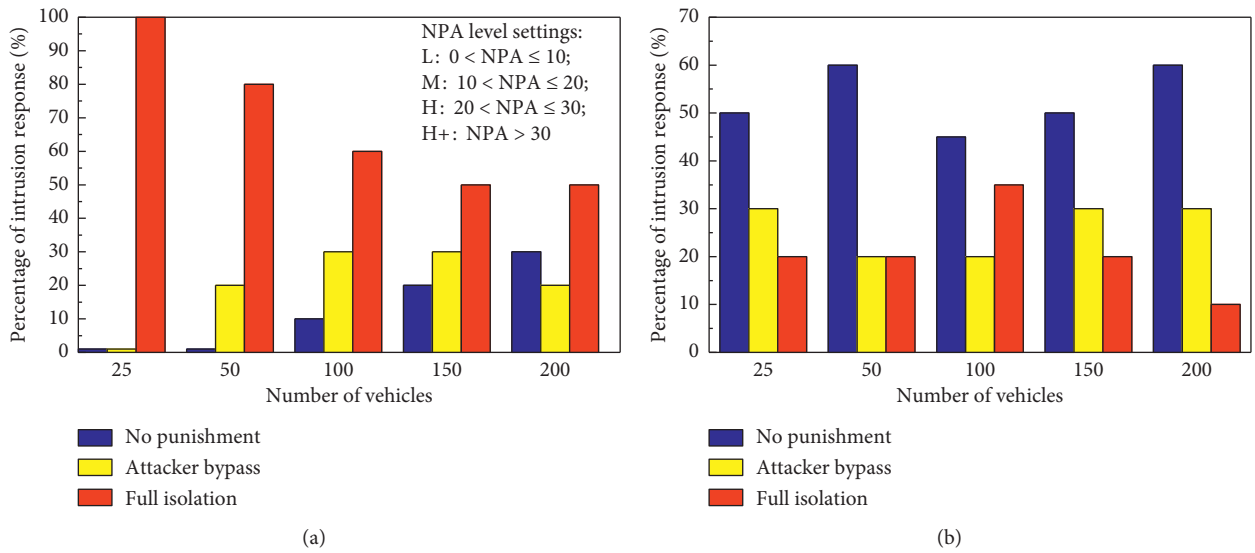

Figure 4: Selection of intrusion response by SD-EPM in attacks. (a) Black hole attack. (b) Rushing attack.

4.1.2. Efficient Response. The intrusion response behavior selected for an efficient response is shown in Figure 4. The SD-EPM selects full isolation to respond to the intrusion in most cases in black hole attacks. Full isolation is selected in the case of an average of 90% in the small networks consisting of 25 and 50 vehicles; full isolation is selected in the case of an average of 54% in the large networks consisting of 100, 150, and 200 vehicles. This is because black hole attacks are a serious attack, and selecting full isolation to treat intruders as nonexistent will significantly improve the overall network performance. However, the SD-EPM selects no punishment in most cases in rushing attacks, which has nothing to do with the dimension of the network. Rushing attacks have less damage to the network. If it is full isolation or attacker bypass under weak attack conditions, the network performance will be attenuated. Overall, the data results show the flexibility and effectiveness of the SD-EPM.

4.2. Impact of SD-EPM on Network Performance. NPA is used as a metric to analyze the effectiveness of SD-EPM in four different attacks and their combined attacks. The proposed mechanism is compared with the two typical protection mechanisms: GIDP [17] and SRM [18]. The effectiveness of SD-EPM in a network consisting of 25 vehicles and 50 vehicles, respectively, is shown in Figure 5. It can be seen from the figure that the SD-EPM has the least impact on NPA. In the network of 25 vehicles, the NPA with SD-EPM (efficient response) is 4% (average) lower than the GIDP

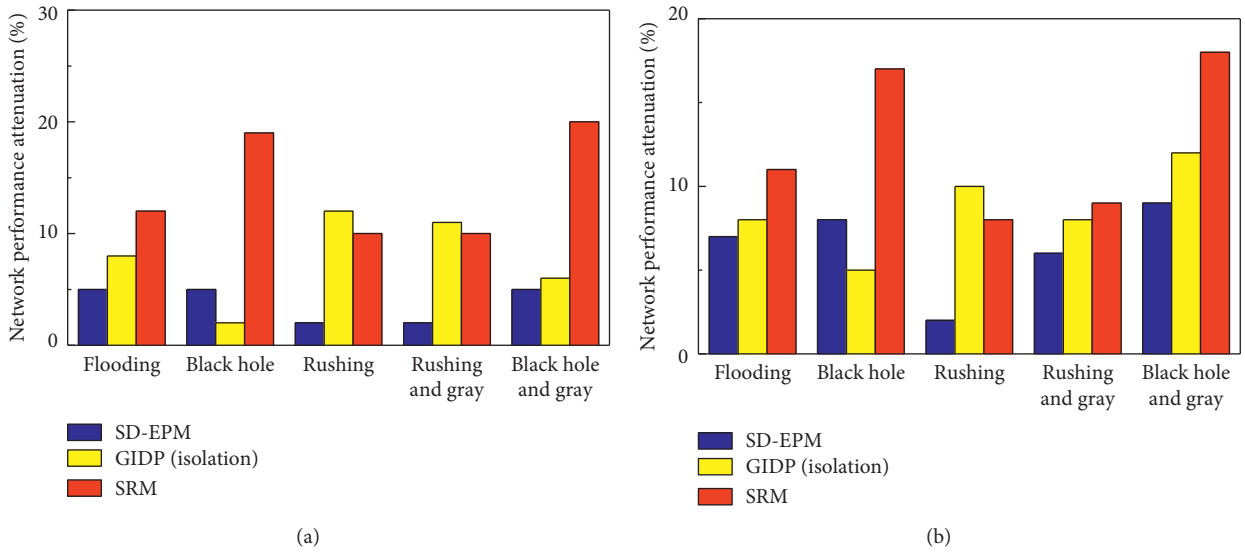

Figure 5: Effectiveness of the intrusion response. (a) 25 vehicles. (b) 50 vehicles.

(fixed intrusion response) and 10.4% (average) lower than the SRM (no intrusion response). In the network of 50 vehicles, the NPA with efficient response is 2.2% (average) lower than the GIDP and 6.2% (average) lower than the SRM. The results show that SD-EPM not only minimizes the negative impact of network performance on all attacks, but also significantly reduces the negative impact on network performance in a minor attack like a rushing attack.

5. Conclusions

This paper proposes an efficient protection mechanism for vehicular ad hoc networks in urban areas. Differing from the existing protection mechanisms, the proposed mechanism not only accurately detects attacks, but also provides appropriate responses to different attacks to prevent attacks. SD-EPM shows the importance of self-adaptive decision in different attack scenarios. Based on the AC and NPA, the self-adaptive decision list is used as the selection criterion of the intrusion response behavior to realize the maintenance for network security of autonomous vehicles. Technical guarantee for the security application of the future VANETs is provided.

Abbreviations

VANETs: Vehicular ad hoc networks
NPA: Network performance attenuation
AC: Attack credibility
OBU: On-board units
CAM: Cooperative awareness message
PKI: Public key infrastructure
ID: Identification
RFID: Radio frequency identification
CA: Certificate authority
RSU: Road side unit
CAN: Controller area network
IDS: Intrusion detection system
DoS: Denial of service
T: Time interval
VN: Vehicle node
CVN: Central vehicle node
NM: Network matrix
PM: Performance matrix
MVN: Management vehicle node
IP: Initial profile
TSW: Test sliding window
RB: Responding behavior.

Data Availability

The data used to support the findings of this study are currently under embargo, while the research findings are commercialized. Requests for data, 12 months after publication of this article, will be considered by the corresponding author.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (61771186), University Nursing Program for Young Scholars with Creative Talents in Heilongjiang Province (UNPYSCT-2017125), Distinguished Young Scholars Fund of Heilongjiang University, and Postdoctoral Research Foundation of Heilongjiang Province (LBH-Q15121).

References

[1] S. Bitam, A. Mellouk, and S. Zeadally, "Bio-inspired routing algorithms survey for vehicular ad hoc networks," *IEEE*

Communications Surveys & Tutorials, vol. 17, no. 2, pp. 843–867, 2019.

[2] Y. Yao, B. Xiao, G. Wu et al., "Multi-channel based sybil attack detection in vehicular ad hoc networks using RSSI," *IEEE Transactions on Mobile Computing*, vol. 18, no. 2, pp. 362–375, 2018.

[3] J. Baruch, "Steer driverless cars towards full automation," *Nature*, vol. 536, no. 7615, p. 127, 2016.

[4] A. A. Korba, M. Nafa, and Y. Ghamridoudane, "Anomaly-based intrusion detection system for ad hoc networks," in *Proceedings of the 2016 7th International Conference on the Network of the Future (NOF)*, November 2017.

[5] A. Shabtai, U. Kanonov, and Y. Elovici, "Intrusion detection for mobile devices using the knowledge-based, temporal abstraction method," *Journal of Systems & Software*, vol. 83, no. 8, pp. 1524–1537, 2010.

[6] C. Gong, M. Zhai, and J. Diao, "Research of privacy protection mechanism for vehicles secure communication," in *Proceedings of the 2013 6th International Conference on Information Management, Innovation Management and Industrial Engineering*, November 2013.

[7] K. M. A. Alheeti, A. Gruebler, and K. D. McDonald-Maier, "An intrusion detection system against black hole attacks on the communication network of self-driving cars," in *Proceedings of the 2015 Sixth International Conference on Emerging Security Technologies (EST)*, pp. 86–91, IEEE, Braunschweig, Germany, September 2015.

[8] M. Gmiden, M. H. Gmiden, and H. Trabelsi, "An intrusion detection method for securing in-vehicle CAN bus," in *Proceedings of the 2016 17th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*, December 2016.

[9] K. M. A. Alheeti and K. Mcdonald-Maier, "An intelligent intrusion detection scheme for autonomous vehicles based on magnetometer sensors," in *Proceedings of the 2016 International Conference for Students on Applied Engineering (ICSAE)*, 2017.

[10] K. Selvakumar and N. Seethalakshmi, "Secure group key management protocol for mobile ad hoc networks," *Cluster Computing*, vol. 22, no. 5, pp. 1–7, 2018.

[11] P. Sivaranjanadevi, M. Geetanjali, S. Balaganesh, and T. Poongothai, "An effective intrusion system for mobile ad hoc networks using rough set theory and support vector machine," *IJCA Proceedings on EGovernance and Cloud Computing Services*, vol. 2, pp. 1–7, 2012.

[12] X. J. Tang, "Research of double-path AODV routing algorithm based on energy in Ad Hoc networks," *Information & Communications*, vol. 199, no. 3, 2012.

[13] K. Geetha and N. Sreenath, "Detection of SYN flooding attack in mobile ad hoc networks with AODV protocol," *Arabian Journal for Science & Engineering*, vol. 41, no. 3, pp. 1161–1172, 2016.

[14] N. Jaisankar, R. Saravanan, and K. D. Swamy, "A novel security approach for detecting black hole attack in MANET," *Communications in Computer and Information Science*, Springer, Berlin, Germany, 2010.

[15] J. Sen, M. Chandra, and S. G. Harihara, "A mechanism for detection of gray hole attack in mobile ad hoc network," in *Proceedings of the 2007 6th International Conference on Information, Communications & Signal Processing*, IEEE, Singapore, 2011.

[16] G. Singhchandel and R. Chowksi, "Effect of rushing attack in AODV and its prevention technique," *International Journal of Computer Applications*, vol. 83, no. 16, pp. 10–15, 2013.

[17] A. Nadeem and M. Howarth, "Protection of MANETs from a range of attacks using an intrusion detection and prevention system," *Telecommunications Systems Journal Springer*, vol. 52, no. 4, pp. 2047–2058, 2013.

[18] O. F. Gonzalez Duque, A. M. Hadjiantonis, and G. Pavlou, "Adaptable misbehaviour detection and isolation in wireless ad hoc networks using policies," in *Proceedings of the 2009 IFIP/IEEE International Symposium on Integrated Network Management*, pp. 1–5, IEEE, Long Island, NY, USA, 2010.