IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 15, 2018, accepted September 15, 2018, date of publication October 10, 2018, date of current version October 29, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2875104

A Software Defined Networking-Oriented Security Scheme for Vehicle Networks

RONG GENG[1], (Member, IEEE), XIAOJIE WANG[2], (Student Member, IEEE), AND JUN LIU[1]
[1]School of Computer Science and Engineering, Northeastern University, Shenyang 110819, China
[2]School of Software, Dalian University of Technology, Dalian 116620, China

Corresponding author: Jun Liu (liujun@cse.neu.edu.cn)

This work was supported in part by the National Natural Science Funds of China under Grant 61701100, Grant 61501038, and Grant 61671141, and in part by the Fundamental Research Funds for the Central Universities under Grant N161613001.

ABSTRACT In the intelligent transportation system (ITS), vehicle networks (VNs) can well solve the network related problems. However, as VNs are expected to have a wide range of applications in future services, security challenges are widely recognized. Consequently, security solutions for VNs are urgently needed. In this paper, we propose a new security strategy for VNs. We first construct the network architecture for VNs through the software defined networking. The security schemes are then embedded in the protocol to defend the common security attacks in the network. Moreover, in order to meet the security requirements of different data and computation overhead, several security schemes are studied for anti-replay, anti-eavesdropping, anti-tamper, anti-wormhole, and anti-forger, through the selection of packets to choose different modules. In particular, we focus on the anti-replay security scheme and use sequence number algorithm and MAC complete sequence number method in master and multi-service modules, respectively. The security schemes are simulated and analyzed by NS-2, which shows that the performance of the proposed security schemes is superior in terms of packet delivery ratio, average end-to-end delay, and control overhead.

INDEX TERMS Vehicular networks, security scheme, software defined networking.

I. INTRODUCTION

In the intelligent transportation system (ITS), Vehicular networks (VNs) are becoming the most promising research topic, because they provide comfortable and safe information for drivers and passengers [1]–[3]. They are distributed and self-organizing networks composed of many high-speed vehicles. As one of the most valuable type of MANETs, VNs make security and privacy issues a real challenge because of the characteristics especially the communication in open access environments [4].

For the security of VNs, the network nodes are prone to capture, tamper and interfere from the attackers, and the messages between nodes can be eavesdropped and fake messages are injected or replayed into the network. Malicious nodes deliberately interfere with the normal behavior of the network, aiming at disrupting the normal functionalities of the network. These problems may affect the large-scale deployment of VNs. Therefore, the security problem of the VNs is a hot research topic [5]–[7].

Software-Defined Networking (SDN) [8]–[10] is considered promising to simplify network management, and the research innovations are based on the decomposition of the control and data planes. It is especially required for VNs to be highly flexible to adapt to any situation and use case, and to provide very low latency. Thus, it needs to be reconstituted to break through the traditional network structure and simplify hardware function [11]–[13].

Aiming at the problems mentioned above, we propose a novel security strategy for VNs in this paper. A network architecture is first constituted by software defined idea. In the designed network architecture, the network is divided into four layers: namely, infrastructure layer, virtual layer, control layer and application layer. On this basis, the security schemes are embedded in the control layer. Furthermore, in order to meet different security requirements with different packets, we provide different security schemes in the master module and multi-functional module in control layer. The packets can choose appropriate security protection according to the network state and requirement. Our main contributions of this paper are demonstrated as follows:

- We constitute the network architecture for VNs based on the idea of software defined networking to simplify network management.

- The security schemes are embedded in the control layer, such as anti-replay, anti-eavesdropping, anti-tamper, anti-wormhole, anti-forger, so that the packets can choose the appropriate security protection according to the network state and requirement.
- We present several different security schemes to provide different security requirements. And we focus on the anti-replay security scheme using sequence numbers algorithm and MAC complete sequence number method respectively in master module and multi-service module. In the anti-replay security schemes as an example, we present the two schemes in detail.

The rest of this paper is organized as follows. In Section II, we illustrate the related works of the existing security policies including network coding, reputation, the combination of active and passive response and cryptography. In Section III, the security schemes are proposed for VNs, which consist of the hierarchies of the networks, based on software defined idea and embedded security schemes. Section VI demonstrates the simulation results, and our work is concluded in Section V.

II. RELATED WORK

In the wireless networks, it needs to adopt security policies that help bring their risks to a manageable level. Some existing common security policies are mainly the following:

1) SECURITY POLICY BASED ON NETWORK CODING

Network coding [14]–[18] realizes the transformation from classical store-and-forward routing to information flow. This new code-and-forward paradigm considers that the source messages are algebraic entities upon which operations can be performed at the intermediate nodes. Network coding can increase the discrete nature of data information, the network encryption and crack difficulty, and can also improve network security performance. Deterministic network coding can improve the security of the system even if its transmission node number is large, through the appropriate network coding. Thus, different network performances choose different network coding, is the first need to consider the problem of wireless network coding. Chen *et al.* [14] proposed a distributed detection algorithm against wormhole in wireless network coding systems, which can detect the malicious nodes participating in wormhole attack. Cai and Yeung [15] considered that an eavesdropper is allowed to access a subset of network channels without being able to obtain information transmitted for unicasting. The work in [16] presented the key security mechanisms of network coding as well as a detailed analysis of the security goals and threats. Le *et al.* [17] focused on eavesdropping attacks and used random linear network coding to reduce the number of encryption operations. Liu and Du [18] relied on network coding to provide data confidentiality, and the scheme can resist a series of attacks suffered in wireless Ad Hoc network, such as eavesdropping attack.

2) SECURITY POLICY BASED ON REPUTATION

Some evaluation of security policy also focused on the principles of reputation [19]–[21]. Reputation is the perception that the peers form about a node. In [19], the reputation-based framework employed direct observation and second-hand information distributed among a network to evaluate other nodes. Wang *et al.* [20] took both information and path correlation into consideration and evaluated the reputation of nodes in a feedback manner. Generally speaking, reputation is used to evaluate security with numerical and computational mechanisms. By reputation evaluation the routing security metric was compared with the standard value, the new metric with part of the security information would be obtained and weighted though the metric by comparing traditional routing protocol metric. In [21], a trust-based probabilistic recommendation model for social networks was proposed and analyzed the impact of the transition probability influence factor through experiments.

3) SECURITY POLICY BASED ON THE COMBINATION OF ACTIVE AND PASSIVE RESPONSE

Intrusion detection system [22]–[25] can be divided into two modes: active response and passive response. For the collected unnormal information, the former is likely to control the attacked system, block or mitigate the impact of the attacks. However, the latter only sends an alarm notification, instead of fighting back to the attacker. Through scheduling network information based on the reputation mechanism, the intrusion detection system would actively protect the network dynamic security, effectively defense against malicious nodes. In order to evaluate network nodes, the research of accurate reputation of nodes will achieve mutual supervision between nodes in the network. Through the research of the hidden and latent of the malicious attacks, we can choose different security policies for the nodes, and take the measure based on the combination of initiative and passive to protect the undeniability and integrity of the wireless network.

Obimbo *et al.* [22] allowed the participating nodes to listen to the nodes they have transmitted messages to. If the message is not relayed within a certain time, the node is suggested to be tagged as a misbehaving node and can be used in determining the route for sending package. In [23], the nodes that have highest trust value, residual bandwidth and energy could be the active nodes. Each active node monitored its neighbor nodes within its transmission range and collected the trust value from all monitored nodes. Each active node with highest trust value, residual bandwidth and residual energy monitored its neighbor nodes within its transmission range, and collected the trust value from all monitored nodes. Below the minimum trust threshold, the node is marked as malicious. When the source node receives alert message about the malicious node, a defense technique is deployed to filter the corresponding malicious node from the network. Similar monitoring methods have also been used in [24]. The method in [25] employed fault tolerance techniques and cryptographic mechanisms to detect and deal with malicious or faulty nodes.

4) SECURITY POLICY BASED ON CRYPTOGRAPHY

In wired and wireless networks, cryptography [26]–[28] is generally utilized to ensure the information confidentiality. In [26], the Advanced Encryption Standard (AES) was introduced in the route selection phase to strengthen the integrity of the data while securing the potential routes chosen for data transfer from source to destination nodes. An identity-based key management and authentication system was proposed in [27], [28] for MANET, using identity-based and threshold cryptography.

The secure policies of above mentioned can solve some security problems, but VNs need to be reconstituted to break through the traditional network structure and simplify hardware function. Therefore, in this paper, we first construct VNs based on the main idea of software defined networking, and change the hierarchical structure aiming to reduce the network hierarchical overhead. Aiming at the possible security problems for VNs in the routing process, multi-modules protocol is embedded with security structure. For different security attacks, different security schemes have been proposed, and data packets can choose appropriate modular according to the network status and security requirements. Then the security option identifier is added to the packet header, to solve the data packet security defense requirements with the most reasonable overhead.

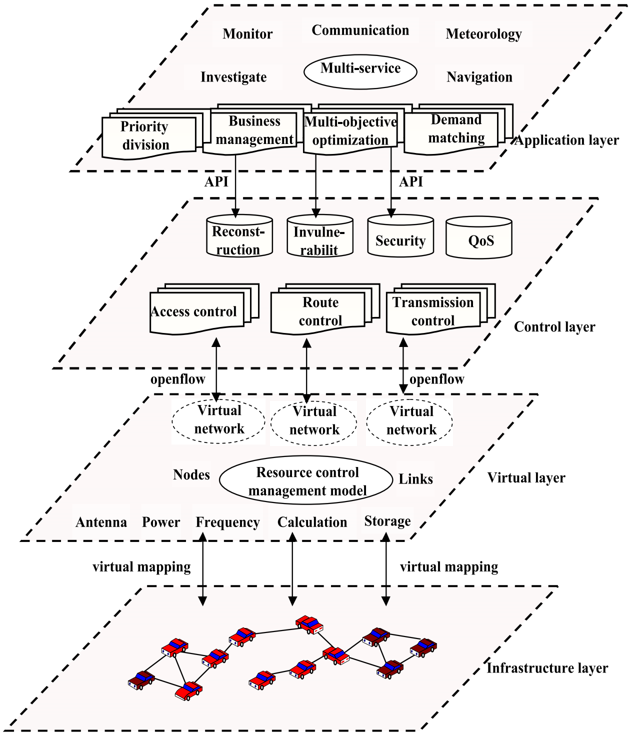


FIGURE 1. The network architecture of VNs.

III. SYSTEM DESIGN

In this section, we first constitute the network architecture based on software defined idea. Then, several security schemes are embedded in the protocol to defense the common security attack in the network such as replay, anti-eavesdropping, tamper, wormhole, and forger. And we describe in detail the sequence numbers algorithm and MAC complete sequence number method for replay attack.

A. NETWORK STRUCTURE

Given the heterogeneity of VNs, it is challenging to coordinate and optimize the use of heterogeneous resources with the goal of satisfying as many services as possible. The network structure is based on the idea of software defined networking, and simplifies hardware function, where the network is divided into four layers: infrastructure layer, virtual layer, control layer and application layer. SDN architecture can use the OpenFlow protocol to manage the infrastructure in the VNs network and use the OpenFlow protocol to implement the basic functions. As shown in Fig. 1, Infrastructure layer is the lowest level which is used to manage the vehicles. The SDN structure strips out the control function of the underlying information, so that what the vehicles should do is clear and single: receive data flow, forward according to protocol, and no longer care about a series of decision-making problems in the network. Virtual layer is the lower layer which is designed to turn distributed network into virtual centralized network for routing security. Control layer is the higher layer, and it decides which networks should be used for application flows and how application flows should be routed across the network. Furthermore, control layer is employed to achieve routing security. Application layer is the highest layer of structure in networks that define what is required and is utilized to achieve multi-functional module. The separate abstraction layers allow dedicated algorithms to be designated to a certain layer for improved performance.

1) INFRASTRUCTURE LAYER

Software defined networking allows for a clear separation of concerns between services in the control plane and the data plane. Therefore, we hide the details of network devices so that the service can be accomplished in more flexible way by adding Openflow switcher. Openflow switcher completes basic switch through node control. In the infrastructure layer, the heterogeneous devices exploit different data formats for modeling information and diverse protocols, so they need to be virtualized by the upper virtual layer.

2) VIRTUAL LAYER

Virtual layer is a logical layer instead of physical connection, including virtual controller and virtual user manager. VNs includes all kinds of nodes that are required to make virtualization through virtual layer. If multiple virtual networks are allowed in the same physical network, we can regard this network environment supports network virtualization. Every virtual node in virtualization environment is composed of many nodes and links. In essence, the virtual layer is a subset of the lowest physical network.

3) CONTROL LAYER

Control layer is an implementation layer of secure routing in VNs. In VNs, a massive number of devices connected to the Internet and the huge data associated with it, so there remain concerns about the security. It is difficult to guarantee their security by traditional methods, since the network status should be considered, and the security schemes should be chosen. Once the network is attacked, the network performance would be reduced, or even the whole networks would be failed. Therefore, it is necessary to analysis the security vulnerability of routing protocols and to adopt multi-strategy security, which is embedded in the protocol by using multi-modules. There are different security requirements with different packets, so we provide several different security schemes in the master module and multi-functional module, and the packets can choose the appropriate security protection according to the network state and requirement.

4) APPLICATION LAYER

Application layer is used to handle various kinds of applications. When a packet transfers from the lowest layer to the highest layer, the whole routing is completely transparent to the applications, thus the implementation of these applications need software programming. When a packet is sent to the application program modules, the packet is queued into the calling application, then the system deals with it according to its service requirement.

Through each layer above mentioned, we apply the idea of software defined networking in VNs to reduce restrictions on network hardware and simplify hardware features. The information transmission, security, traffic analysis and other network functions can be defined by software to improve flexible configuration, reconstruction, renewal and upgrade capability of VNs. Through multi-functional interface, the applications can achieve the corresponding functions. Packet tunnel encapsulation and reduction of software flow table lookup can solve the problem of the security routing protocol difficult for implementation. Dynamic trust management can be embedded in the network management for network behavior and services requirement, which can protect the security issues such as route established, software implementation, data collection and so on.

For example, consider a specific instance of sending special military command. Once such a task is submitted to application layer from a requesting node, the applications can achieve the corresponding functions through a series of steps:

- The application will identify the security through multi-service interface to control layer. Some security options are added into the packet header section, which contains the security types.
- In other nodes received the packets, data packets transfer from lower layer directly into the master module of control layer, then the module make a judgment on security option. When security option indicates the option with simple way, it will stay here. When security option indicates the option with senior way, it will go into multi-functional module from master module. If the packets require anti-replay protection, multi-functional module is called by master module to carry enhanced security protection with higher overhead.

B. SECURITY PROTECTION SCHEMES

Because VNs is made of all kinds of devices, and some devices are resource-constrained nodes, it is necessary to guarantee the network security while minimizing overhead as much as possible. The multi-modules security requirement choice for network state and service requirement is designed in this paper. Some security options are added into the packet header section, which contains the security types and the five security options.

Security protection can be divided into master module and multi-functional module. The common problems are usually handled in the master module with most packets, and in multi-functional module, external applications are called to provide comprehensive maintenance for security assurance. According the current network state and requirement, source node makes module selection.

In the control layer, data packets transfer from lower layer directly into the master module, then the module make a judgment on security option. When security option indicates the option with simple way, it will stay here. When security option indicates the option with senior way, it will go into multi-functional module from master module. The judgment of security level is usually based on security environment of communication, conditions and security of data packet itself. Through the choice of modules, security overhead will be effectively reduced.

1) MULTI-MODULES SECURITY DESIGN

In the design scheme, the security option identifier is added into the packet header, as shown in Fig. 2. Firstly, the security bit is judged. If the security bit is set to 0, the packet does not need security protection and the security bit is set to 1, then all the bits behind will continue to be judged.

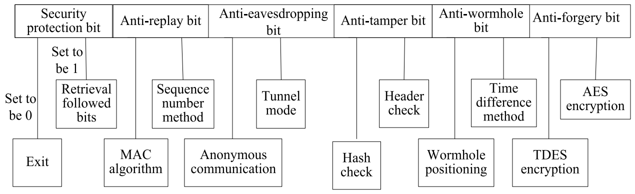


FIGURE 2. Security option bit design diagram.

The following five bits represent the different means of protection for security problems more prone to happen in VNs. If the required security protection is not high level with low overhead, the security algorithm in the master module is used, and if the packets require special protection, multi-functional module is called by master module to carry enhanced security protection with higher overhead. In the following, the details of the security option will be introduced.

a: ANTI-REPLAY BIT

In the master module, only a counter is added. When a packet has been transmitted to the master module, the rest four bits of the sequence number in it are extracted and compared. If they are same, the data packet is considered to be normal, and the counter is incremented. Otherwise, it would be sent to multi-functional module. In the multi-functional module, the packet will be judged whether it is a replay packet or a packet with discontinuous sequence number that previous packet was lost. The calculation scheme is added into the multi-functional module and the packet will be judged by the MAC complete sequence number method of replay attack. If the packet passes the validation, it should be a packet with discontinuous sequence number, and simultaneously its serial number will be returned to master module counter in order to check next packets.

b: ANTI-EAVESDROPPING BIT

In the master module, the packet will be checked whether it needs to prevent eavesdropping and use the tunnel mode to reduce the computational overhead. By adding a new IP header, the tunnel mode achieves security features. The IP header contains the version identifier, the header length, the protocol ID, control field, a parity bit of source and destination addresses, the basic QoS guarantee field, and header check sum field.

When the anti-eavesdropping bit in multi-functional module shows a reminder about transmission overhead, the packet is sent to the multi-functional module to be processed by the anonymous communication model to block, splicing, and ultimately achieve the demands of the anti-wiretapping. The anonymous communication mode includes three steps: fragmented processing and network coding in source node, forwarding in intermediate node, and decoding in destination node.

c: ANTI-TAMPER BIT

In the master module, only the parity check is done to simply compare anti-tamper bit instead of tamper check. If it has high security level requirements, the packet will be transmitted into the multi-functional module and make identification according to the MAC integrity hash check module.

d: ANTI-WORMHOLE BIT

In the master module, time difference algorithm is used. Only a single counter is added to calculate the Round-Trip Time (RTT), and then the value is divided by the hops. If it meets the certain threshold, it is considered as a security packet. Otherwise, it will be transmitted into the multi-functional module. In the multi-functional module, the packet will be checked to decide whether it is a wormhole packet or the processing time for packet within a certain node is too long. Wormhole localization algorithm is used to detect malicious nodes and then further to find out whether there is an abnormal topology.

e: ANTI-FORGERY BIT

In the master module, only the head encryption system is added to compare the anti-forgery bit based on the AES encryption. If it has high security level requirement, the packet will be transmitted into the multi-functional module and to make encryption and decryption according to the requirement of the packet.

According to the requirement, several different security schemes are proposed in the paper according to different security attacks. In the following part of our work, we will detail the two kinds of schemes with the anti-replay security schemes.

2) ANTI-REPLAY ALGORITHM

a: SEQUENCE NUMBER ALGORITHM

Sequence number algorithm is called the simplified security scheme. The key to prevent the replay attack is to ensure the ‘‘freshness’’ of the message, so that the message exists in a certain period of time. The simplest method is to compare the sequence number of the message by the receiver to determine whether the message is new or replayed. In general, this method requires that each pair of communicating entities store a pair of sequence number which can be used to detect the message ‘‘freshness’’. After the entity receives the message, the sequence number will be checked whether it is valid according to the policy prior consultation. In this way, because each message has its own different sequence number and is not repeated, the receiver can distinguish between old and new messages. However, the sequence number does not have the anti-forgery means.

b: MAC COMPLETE SEQUENCE NUMBER METHOD

MAC complete sequence number method is used in the multi-functional module. The security model of the MAC complete sequence number method is shown in Fig. 3.

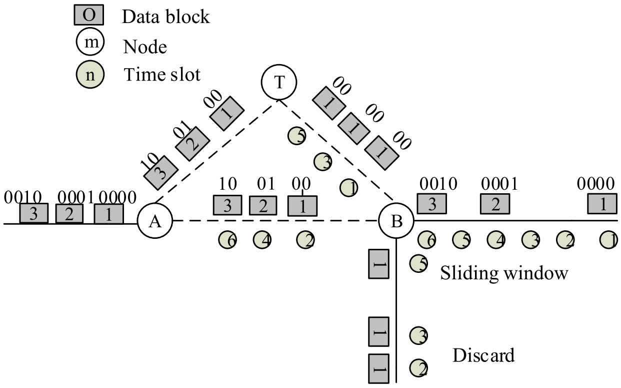


FIGURE 3. Mode figure of security mechanism.

For the discontinuity problem of sequence number caused by packet loss, it does not need to be verified by successively plus 1 to sequence number, and only validated in high (n-m) bit by successively plus 1. However, when receiving an error message or an illegal message sent by an attacker, the validation with the method of high ((*n*-*m*}) bit by successively plus 1 would never succeed. Thus, the threshold value is defined to be a threshold of authentication times, and is set to

$$\theta = |L/2^m| \tag{1}$$

where L is the maximal value of continuous packet loss in the network. When the receiver is continuously verified times, it will be discarded directly. In the process of continuous messages verification, the efficiency of the MAC complete sequence number is $2m$ times that of the window mechanism. The packet disorder problem may be happened in VNs because of packet loss, multipath, dynamic topology and other factors, so the adaptive window of the MAC complete sequence number method can effectively reduce the error rate. In addition, the MAC complete sequence number method can be anti-forgery, while the sequence number algorithm cannot be.

IV. SIMULATION RESULT

In these experiments, the performance of the security protection is evaluated in terms of the following metrics of interest:

Packet delivery ratio: it is defined as the proportion between the amounts of packets received by receivers and the received number of data packets, which illustrates effectiveness of the security schemes.

Control overhead: it is measured as a ratio of the number of control bytes generated by nodes across the network to the total number of data bytes sent by the source node.

Average end-to-end delay: it is defined as the delay of packet delivery and contains propagation, queuing and transfer delays.

We customized NS with soft defined networking features by injecting an OpenFlow-like protocol in IP layer [29]–[32]. In every network scenario, there is only one node serving as the cluster head node with strong computing ability, and the remaining nodes are all controlled node. Application requirements, network topology and device properties are registered to the cluster head node.

In this section, three different security schemes (i.e., Normal network without security, Sequence number algorithm-based scheme and MAC complete sequence number method-based scheme) are implemented on the basis of NS-2 in VNs.

The network consists of 50 Vehicles in the simulation, as shown in Fig. 4. When building a route, replay attack is carried out to observe performance changes in the network. In simulation Scene 1, the connections are set to be 6, 12, 18, 24, 30, and the flow rate is always 3 packets/s. Nodes 2 and 15 are malicious nodes for replay attacks, and the packets sent to neighbor nodes is replayed and forwarded. The attack is simulated under the cases of three security levels.

In simulation Scene 2, the number of the malicious node is set to 2, 4, 6, 8, 10, and they replay and forward the packets sent by their neighbors. The number of connections is 24, and the flow rate is set to be 3 packets/s, respectively. The attack is simulated under the cases of three security levels.

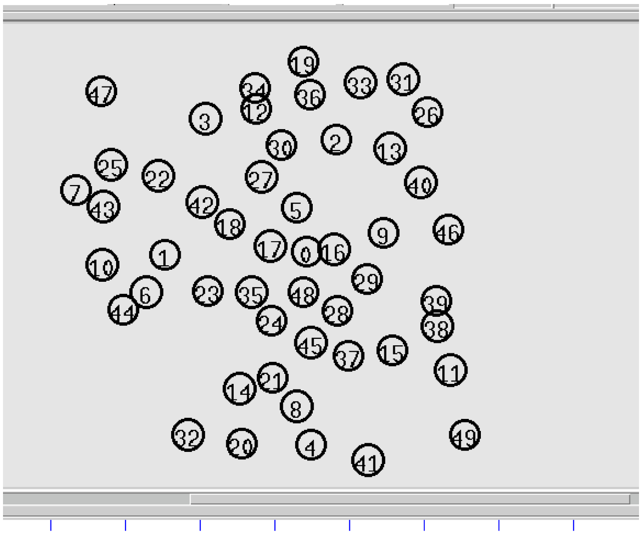


FIGURE 4. Simulation scene topology.

ANTI-REPLAY SIMULATION

Replay attack is also known as rebroadcast attack, playback attack or fresh attack, which means the packet sent by the attacker has been received by destination node to cheat the system, mainly for the identity authentication process and to destroy the correctness of authentication.

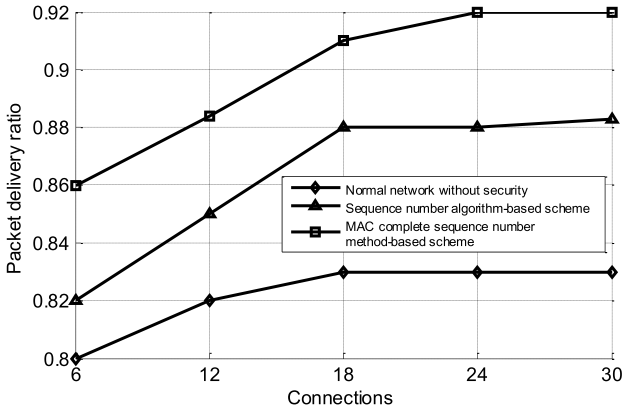


FIGURE 5. The comparison of packet delivery ratio with different connections.

Figs. 5, Fig. 6, Fig. 7 demonstrate the performances of different security levels. The connections vary from 6 to 30 during the simulation time. Fig. 5 and Fig. 6 show that the packet delivery ratio and average end-to-end delay increase as the connections increase. The two figures show that the performances of sequence number algorithm-based scheme and MAC complete sequence number method-based scheme are better than that of the normal network without security scheme. This is because the malicious nodes forward route request constantly, and the bandwidth of routing protocol

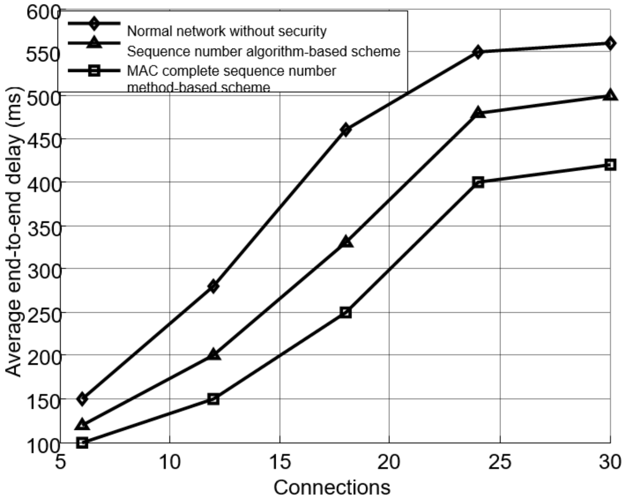


FIGURE 6. The comparison of average end-to-end delay with different connections.

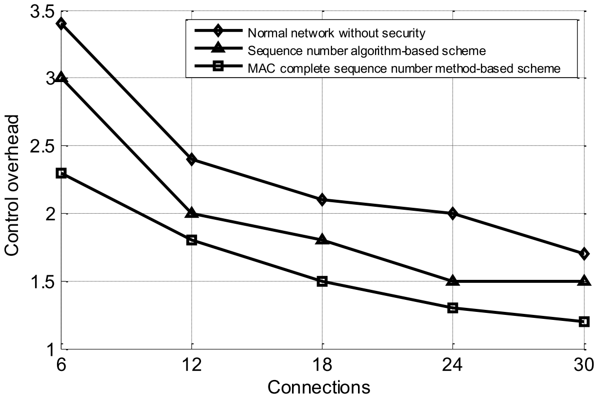


FIGURE 7. The comparison of control overhead with different connections.

is occupied. Therefore, other nodes have no enough network resource to normally carry out route establishment, maintenance and transmission, so that packet delivery ratio of the network is obviously reduced. However, in the MAC complete sequence number method-based, because the malicious nodes and replay packets can be found instantly. The network route can be established, and packet delivery ratio is higher than normal network without security, and the average end-to-end delay is lower than normal network without security. The performance of the sequence number algorithm-based scheme is not as well as that of the MAC complete sequence number method-based scheme because the sequence number needs return to zero periodically in the sequence number algorithm-based scheme. When the nodes receive packets, whose sequence number is smaller than the original one, these packets are considered to have been processed and then discarded. However, in the period of time after each zero, the sequence number of normal packet is less than the replay packet, it is seen as an attack and the normal packet is discarded. Thus, the packet delivery ratio and average end-to-end delay are affected.

Fig. 7 shows that the control overhead varies with the increase number of the connections. When the number of connections increases from 6 to 30 pairs, the control overheads of the three schemes decrease, which is because the control packets increase slowly compared with the data packets and the corresponding ratio decreases. Although MAC complete sequence number method-based scheme adds control packets during security protection, its overhead is still lower than others. This is because when the replay node eavesdrops the packets, it heavily broadcasts the attack information, and a large amount of useless route request information would be forwarded in the network, which heavily increases the overhead and congestion of the network. However, according to the MAC complete sequence number method, reply attack can be verified by the MAC hash so that the reply data packets can be distinguished, and malicious nodes can be rapidly detected. At the same time, the malicious node can be insulated and the useless packets are discarded, thus network transmission overhead can be saved. In the detection process, compared with the large amount of routing overhead caused by the replay attack, the control overhead of the MAC complete sequence number method is negligible, thus the control overhead of the MAC complete sequence number method is significantly less than that of the non-protection scheme.

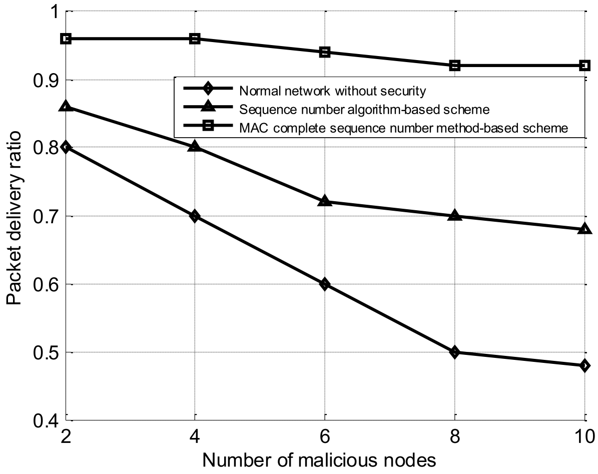


FIGURE 8. The comparison of packet delivery ratio with different number of malicious nodes.

Fig. 8, Fig. 9, Fig. 10 show the performance of three schemes as the number of malicious nodes varies. Although our proposed security schemes can provide good delivery ratio, MAC complete sequence number method has better performance than the other schemes, especially in the scenarios where the number of malicious nodes is larger than 4. In no security scheme, the malicious nodes forward route request constantly, and the bandwidth of routing protocol is occupied, and other nodes have no enough network resource to normally carry out route establishment, maintenance and transmission, therefore packet delivery ratio of the network is obviously reduced, average end-to-end delay and control

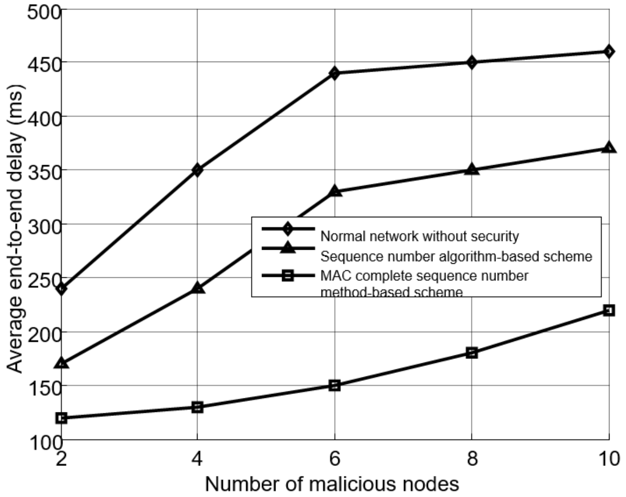


FIGURE 9. The comparison of average end-to-end delay with different number of malicious nodes.

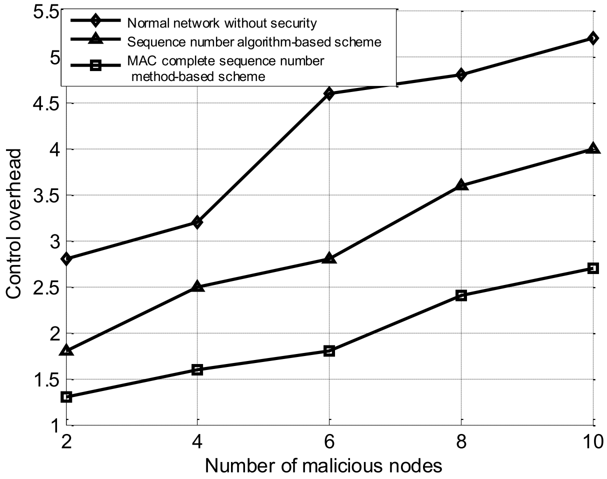


FIGURE 10. The comparison of control overhead with different number of malicious nodes.

overhead are all increased. In our analysis, it is proved that in the MAC complete sequence number method, the malicious node can be insulated, and the useless packets can be discarded. The packet disorder problem may be happened in VNs because of packet loss, multi-path, dynamic topology and other factors, so the adaptive window of the MAC complete sequence number method can effectively reduce the error rate. The performance of the sequence number algorithm is affected because the sequence number needs to be returned to zero periodically in the sequence number algorithm.

V. CONCLUSION

In this paper, we have proposed two novel security strategies for VNs. Firstly, the hierarchies of the network are constituted by software defined idea to simplify network management and decompose the control and dataplanes. On this basis, several different security schemes are embedded into the protocol to defense the common security attack in the network, and to ensure the security and effectiveness of routing process in VNs. Therefore, data packets can choose appropriate modular according to the network status and security requirements. In anti-replay security scheme, we use sequence number algorithm in the master module and MAC complete sequence number method in multi-functional module respectively. Simulation results illustrate that the security schemes can considerably achieve better network performance in terms of network throughput and control overhead compared with normal network without security the network load capacity varies, which have demonstrated the effectiveness of our proposed method.

At present, the proposed security schemes are basically added on the basis of the traditional cryptography schemes. In the future, we will consider using network coding to realize the encryption of information, so as to reduce the overhead and increase the security. In the other hand, although these schemes realize the defense of traditional security issues, new network security problems will arise because of the introduction of the idea of software defined network. While optimizing the network, relevant researches on security risks introduced by software structure should be considered in the next stage. Moreover, these schemes are mainly based on the research on security. In the future work, the correlation of other layers needs to be studied, and the security algorithm supporting adaptive and multi-level joint optimization is designed and implemented.

REFERENCES

[1] J. Li *et al.*, "Most influential community search over large social networks," in *Proc. IEEE Int. Conf. Data Eng.*, vol. 4, 2017, pp. 871–882.

[2] Z. Ning, P. Dong, X. Kong, and F. Xia, "A cooperative partial computation offloading scheme for mobile edge computing enabled Internet of Things," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2018.2868616.

[3] X. Wang, Z. Ning, and L. Wang, "Offloading in Internet of vehicles: A fog-enabled real-time traffic management system," *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4568–4578, Oct. 2018.

[4] Y. Zhang, R. Yu, S. Xie, W. Yao, Y. Xiao, and M. Guizani, "Home M2M networks: Architectures, standards, and QoS improvement," *IEEE Commun. Mag.*, vol. 49, no. 4, pp. 44–52, Apr. 2011.

[5] W. Hou, Z. Ning, L. Guo, and X. Zhang, "Temporal, functional and spatial big data computing framework for large-scale smart grid," *IEEE Trans. Emerg. Topics Comput.*, to be published, doi: 10.1109/TETC.2017.2681113.

[6] L. Guo, Z. Ning, W. Hou, B. Hu, and P. Guo, "Quick answer for big data in sharing economy: Innovative computer architecture design facilitating optimal service-demand matching," *IEEE Trans. Autom. Sci. Eng.*, vol. 15, no. 4, pp. 1494–1506, Oct. 2018.

[7] Z. Ning, X. Kong, and F. Xia, "Green and sustainable cloud of things: Enabling collaborative edge computing," *IEEE Commun. Mag.*, to be published, doi: 10.1109/MCOM.2018.1700895.

[8] B. A. A. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka, and T. Turletti, "A survey of software-defined networking: Past, present, and future of programmable networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1617–1634, 3rd Quart., 2014.

[9] S. Maharjan, Q. Zhu, Y. Zhang, S. Gjessing, and T. Basar, "Dependable demand response management in the smart grid: A Stackelberg game approach," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 120–132, Mar. 2013.

[10] J. Li, T. Sellis, J. S. Culpepper, Z. He, C. Liu, and J. Wang, "Geo-social influence spanning maximization," *IEEE Trans. Knowl. Data Eng.*, vol. 29, no. 8, pp. 1653–1666, Aug. 2017.

[11] Y. Zhang, R. Yu, M. Nekovee, Y. Liu, S. Xie, and S. Gjessing, "Cognitive machine-to-machine communications: Visions and potentials for the smart grid," *IEEE Netw.*, vol. 26, no. 3, pp. 6–13, May/Jun. 2012.

[12] W. Hou, Z. Ning, L. Guo, Z. Chen, and M. S. Obaidat, "Novel framework of risk-aware virtual network embedding in optical data center networks," *IEEE Syst. J.*, vol. 12, no. 3, pp. 2473–2482, Sep. 2018.

[13] X. Hu *et al.*, "Emotion-aware cognitive system in multi-channel cognitive radio ad hoc networks," *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 180–187, Apr. 2018.

[14] F. Chen, Y. Wang, D. Wang, and J. Liu, "Weighted partial network coding and its applications in wireless mesh networks," *Wireless Commun. Mobile Comput.*, vol. 13, no. 14, pp. 1281–1294, 2014.

[15] N. Cai and R. W. Yeung, "Secure network coding," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun./Jul. 2002, p. 323.

[16] V. N. Talooki *et al.*, "Security concerns and countermeasures in network coding based communication systems: A survey," *Comput. Netw.*, vol. 83, pp. 422–445, Jun. 2015.

[17] J. Le, J. C. S. Lui, and D.-M. Chiu, "DCAR: Distributed coding-aware routing in wireless networks," in *Proc. 28th Int. Conf. Distrib. Comput. Syst.*, Jun. 2008, pp. 462–469.

[18] J. Liu, R. Du, J. Chen, and K. He, "A key distribution scheme using network coding for mobile ad hoc network," *Secur. Commun. Netw.*, vol. 5, no. 1, pp. 59–67, 2012.

[19] J. Li, R. Li, and J. Kato, "Future trust management framework for mobile ad hoc networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 108–114, Apr. 2008.

[20] X. Wang, K. Govindan, and P. Mohapatra, "Provenance-based information trustworthiness evaluation in multi-hop networks," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Dec. 2010, pp. 1–5.

[21] Y. Wang, G. Yin, Z. Cai, Y. Dong, and H. Dong, "A trust-based probabilistic recommendation model for social networks," *J. Netw. Comput. Appl.*, vol. 55, pp. 59–67, Sep. 2015.

[22] C. Obimbo and L. M. Arboleda-Cobo, "An intrusion detection system for MANETs," *World Academic Publishing*, vol. 112, no. 7, pp. 27–29, 2015.

[23] G. Indirani and K. Selvakumar, "A swarm-based efficient distributed intrusion detection system for mobile ad hoc networks (MANET)," *Int. J. Parallel Emergent Distrib. Syst.*, vol. 29, no. 1, pp. 90–103, 2014.

[24] A. Morais and A. Cavalli, "A distributed intrusion detection scheme for wireless ad hoc networks," in *Proc. ACM Symp. Appl. Comput.*, 2012, pp. 556–562.

[25] P. M. Mafra, J. S. Fraga, and A. O. Santin, *Algorithms for a Distributed IDS in MANETs*. New York, NY, USA: Academic, 2014.

[26] M. S. Obaidat, I. Woungang, S. K. Dhurandher, and V. Koo, "A cryptography-based protocol against packet dropping and message tampering attacks on mobile ad hoc networks," *Secur. Commun. Netw.*, vol. 7, no. 2, pp. 376–384, 2014.

[27] X. Wang *et al.*, "A privacy-preserving message forwarding framework for opportunistic cloud of things," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2018.2864782.

[28] H. Deng and D. P. Agrawal, "TIDS: Threshold and identity-based security scheme for wireless ad hoc networks," *Ad Hoc Netw.*, vol. 2, no. 3, pp. 291–307, 2004.

[29] J. Li *et al.*, "Personalized influential topic search via social network summarization," *IEEE Trans. Knowl. Data Eng.*, vol. 28, no. 7, pp. 1820–1834, Jul. 2016.

[30] Z. Ning, J. Huang, and X. Wang, "Vehicular fog computing: Enabling real-time traffic management for smart cities," *IEEE Wireless Commun.*, to be published, doi: 10.1109/MWC.2018.1700441.

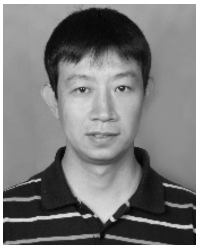
[31] W. Hou *et al.*, "On-chip hardware accelerator for automated diagnosis through human-machine interactions in healthcare delivery," *IEEE Trans. Autom. Sci. Eng.*, to be published, doi: 10.1109/TASE.2018.2832454.

[32] X. Wang *et al.*, "A city-wide real-time traffic management system: Enabling crowdsensing in social Internet of vehicles," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 19–25, Sep. 2018, doi: 10.1109/MCOM.2018.1701065.

[33] W. Hou, Z. Ning, L. Guo, and M. S. Obaidat, "Service degradability supported by forecasting system in optical data center networks," *IEEE Syst. J.*, to be published, doi: 10.1109/JSYST.2018.2821714.

RONG GENG received the B.S. degree in communication engineering, the M.S. and Ph.D. degree in communication and information system from Northeastern University, Shenyang, China, in 2001, 2004, and 2010, respectively. She is currently a Lecturer with Northeastern University. Her research interests are space networks, vehicular networks, network security, and routing.

XIAOJIE WANG (S'16) received the master's degree from Northeastern University, China, in 2011. She is currently pursuing the Ph.D. degree with the School of Software, Dalian University of Technology, Dalian, China. From 2011 to 2015, she was a Software Engineer at NeuSoft Corporation. Her research interests are social computing and network security.



JUN LIU received the degree in communication and information system from Northeastern University, Shenyang, China, in 2008. He is currently an Associate Professor with Northeastern University. His research interests include the space information network, the self-organizing network, and information security.