International Journal of Scientific Research in Science, Engineering and Technology (www.ijsrset.com)
© 2020 IJSRSET | Volume 7 | Issue 3 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
DOI : https://doi.org/10.32628/IJSRSET207387

# SAODV Protocol Based Cryptographic Technique for Automotive Cybersecurity

**Angel Ann G Yesudasan[1], Tressa Michael[2]**

[1]M.Tech Scholar, Department of Electronics & Communication Engineering, Rajagiri School of Engineering & Technology, Ernakulum

[2]Assistant Professor, Department of Electronics & Communication Engineering, Rajagiri School of Engineering & Technology, Ernakulum

## ABSTRACT

This paper presents about a cryptographic technique that is used to ensure cybersecurity in automotive platform. Nowadays there has been a tremendous increase in the number of vehicles which leads to a number of problems like heavy traffic jams. Using Intelligent Transport System, these issues are resolved to a great extent. But using the wireless communication network in automotive give rise to a number of security threats which includes piracy of data and violation of data protection and privacy. To ensure safe and accurate data transmission between the vehicles, there needs to be a cryptographic technique to prevent the attack from malicious nodes. We aim to use SAODV protocol based cryptographic technique which verifies both the source and the destination node of the data transmission process.

**Keywords :** AODV, SAODV, Cyber security, VANET, Black hole attack, NS2 Simulator

## I. INTRODUCTION

Nowadays, the number of vehicles are increasing tremendously. This is leading to a numerous amount of problems like heavy traffic jams, accidents, economical problems as well as air and noise pollution. In order to overcome this problems, the researchers came up with Intelligent Transport System (ITS) [1] which makes use of wireless network technology to enable communication between the vehicles and the base stations. This solution has effectively decreased the problems of traffic jams and reduced the rate of accidents to a great extent.

Obviously now the transportation has become intelligent but there is still a problem when it comes to safety and security of the vehicles and the users. Data privacy and protection of the users comes into scenario when the communication takes place through a wireless network. Attack from malicious nodes like unauthorized users and hackers can intrude into the data and details of the users over the network. Here comes the need of cybersecurity in automotive industry. Basically, Cyber security is essential for communication between the vehicles so that the data is transmitted in the safest way without any intrusion or attack. A number of routing protocols have been developed and implemented to ensure the privacy and protection of data transmitted. Basic protocols give way to a number of loopholes to the attackers to get inside the network. So, we are proposing a modified version of AODV protocol,

termed as Secure AODV (SAODV) protocol for automotive industry as they ensure the security of data transmission by verify both the source and the destination as well as the nodes through which they are travelling in the route. In this paper, we discuss about the need of cybersecurity in automotive industry, the various attacks in the wireless network, working principle of SAODV protocol and the comparison of the protocol with other existing protocol.

## II. NEED OF SECURITY PROTOCOL

A typical vehicular communication network mainly consists of 3 types of communications. They are: Vehicle
to Vehicle, Vehicle to Infrastructure, Infrastructure to Infrastructure [1]. All these communication links needs protection in order to ensure the security of the vehicular data network. Every vehicle will have its own on board units, typically an embedded systems to communicate with each vehicles and road side units that links with the main station. So, we have to ensure an errorless data transmission takes place between all these units without any attacks.

The main concerns of the Intelligent Transport Systems are: (i) Authenticating the information exchange between the vehicles, (ii) To provide accurate information without any errors and (iii) Facing slowness in real time responses. The conventional communication protocols have been facing many security threats in the network as they fail to provide a high throughput in terms of performance and have a huge delay in the data transmission. They are less reliable for a vehicular network. Vehicular wireless networks require real time response and low latency in communication.

For Vehicular Ad-hoc Network (VANET), the main objectives are message authentication and integrity, availability, confidentiality, access control, non-repudiation and privacy [11]. But there are a numerous number of cyberattacks that take place in vehicular network which violates the objectives of VANET [13]. Cyberattacks that cause violation of authentication settings are Sybil attack, impersonation attack, bogus information, session hijacking, replay attacks and GPS spoofing. Attacks that affect network efficiency are denial of service attacks, routing attacks, timing attacks and intruder attacks. Attacks that tamper the privacy of user are eavesdropping and location trailing attack.

Therefore we have to implement a safe and secure lightweight cryptographic technique that will be able to work in an embedded system with less delay and an acceptable performance.

## III. RELATED WORKS

A number of methods have been developed to prevent the attacks in the cyber network. At first, the cyber security was solely concentrated on the Mobile Ad-hoc Networks (MANET) [8]. Various cryptographic techniques like ARAN and SEAD are already successfully implemented in MANETS. But when the security was threatened in MANET, they started developing more protocols that guaranteed more protection to the network data transmission [14]. Similarly as the number of vehicles increased, ITS came into the scenario and VANET was established. But the same security threats faced in MANET is seen in VANET [1] as well.

To improve the security of VANET, protocols like ARAN came at first. Later, protocols like Dynamic Source Routing (DSR) [4] and Destination-Sequenced Distance Vector (DSDV) [4] all came into VANET security network. But they all did have a deteriorated performance when it comes to faster performance because delay in the communication in real time environment is unacceptable, especially for vehicle networks. Then came the AODV protocol [2] which had faster performance compared to other existing protocols. But still, there was a problem with it. The

AODV protocol are prone to black hole attacks and malicious node attacks as many nodes act as false sources and destinations [15]. So we need something more secure in a vehicular platform environment.

## IV. CRYPTOGRAPHIC TECHNIQUE FOR AUTOMOTIVE SECURITY – SAODV

The basic aim in designing the lightweight protocols like AODV [2] and Secure-AODV (SAODV) is mainly to enhance and improve the future automotive security and to meet the security demands of VANET [10]. SAODV is an improved version of AODV which increases the security factor of the protocol. Hash functions are used to estimate the shortest routes and protect hop count and messages are digitally signed to ensure the authenticity of data transmission routes [12]. They make sure the data is sent and received by the authenticated source and destination to avoid the intrusion of a malicious node or a black hole attack.

AODV is basically a routing protocol that does not support the security and privacy of routing messages in the transmission paths [3]. SAODV is an improved version of the AODV routing protocol that is designed to meet the security requirements of the routing messages [9]. The main difference of SAODV from AODV is that they have an extension message in addition to the normal message packet. The extension messages consists of a digital signature of the AODV packet. The digital signature is created from the private key made by the original or authenticated sender of the routing message and a hash based value of the hop count in the data transmission route. Asymmetric cryptography is the basic principle used by SAODV in which all non-mutable fields of the messages are authenticated. The hash function [14] ensure the accuracy in the hop count and in finding the shortest path.

## V. SAODV PROTOCOL WORKING PRINCIPLE

SAODV process mainly is divided into two phases and they are (i) Route discovery phase (Verification Round) and (ii) Route maintenance phase (Verification Confirmation Round). The key feature and main advantage of the SAODV protocol is that it increases accuracy and security of the data route by directly verifying the destination node with the interexchange of some random numbers between the true source and destination.

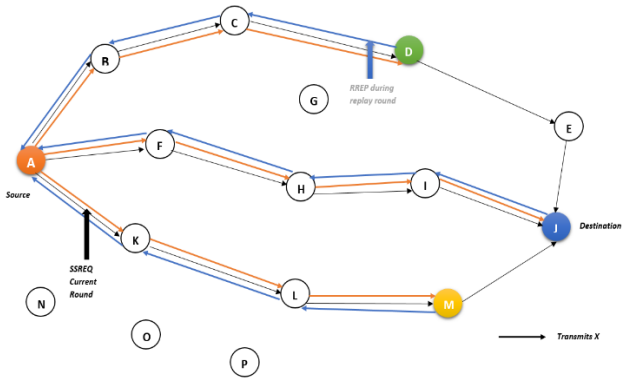


Figure 1: SAODV Protocol – Route Discovery Phase

In figure 1, it depicts the route discovery phase which is also termed as the verification process. The route discovery phase along provides the security features like authentication, integrity and non-repudiation. In the verification process, the destination node is directly verified by the source node by the exchange of random numbers between them. The process starts when the source node 'A' receives a RREP (Route Reply) message packet in the reply round of verification process or route discovery phase. When the source 'A' receives the RREP, it is stored in the routing table and sends a verification message called as SRREQ (Secure Route Request) to the destination via the opposite direction of the same route through which RREP is received to the source 'A'. The SRREQ message packet consists of a random number, let's say 'X', which is generated by the source node. As shown in the figure 1, the black arrow shows the

transmission of random number 'X' starting from source 'A' to destination node 'J'. The destination node stores the SRREQ message in its routing table if it receives at least two SRREQ messages on different data routes. The message content in the routing table is compared to check whether they have the same value as that of 'X'.

Figure 2 depicts the Route maintenance phase. Once the comparison is performed, based on the data obtained, two steps are performed for verification confirmation process which is also termed as route maintenance phase. The first step is to send a verification confirm message known as SRREP (Secure Route Reply) via the opposite direction of the route through which SRREQ is received. Similar to SRREQ, the SRREP also contains a random number, here let's take 'Y' which is generated by the destination. We can see a green arrow in Figure 2 which shows the transmission of 'Y' from destination node 'J' to source node 'A'.

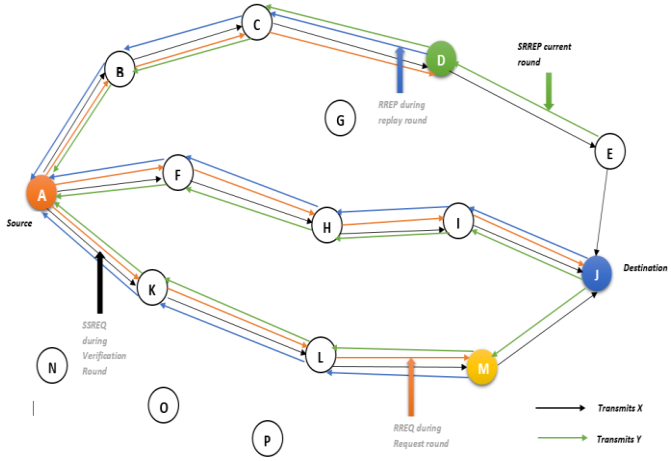


Figure 2: SAODV Protocol – Route Maintenance Phase

Consider an example. In the figure 2, the destination node 'J' received SRREQ messages from the routes through the nodes I, M, and E that have the same value of 'X'. As a result, the destination node 'J' sends a SRREP message with 'Y' to each of the nodes I, M and E as indicated by the green arrows in Figure 2.

The second step is the case which is taken into account when the SRREQ messages have different 'Y' values. In that case, the destination node 'J' needs to wait until it receives at least two SRREQ messages that have the same value as that of 'Y' value and then have to perform the first step. Another scenario is when the source node 'A' receives two SRREP message packets that have the same 'X' value from different routes, it will go for the chooses the route with the shortest number of hops to the destination node 'J'. After selecting the verified and confirmed shortest route to the destination node 'J', the source node 'A' starts its data transmission to the destination.

## VI. EXPERIMENTAL ANALYSIS

The platform that is used for experimental analysis of the routing protocol is NS2 Simulator [4]. As it is an object-oriented and discrete event-driven network simulator, it supports simulation scripts or scenarios, to be easily written in a script-like programming language like tcl. The next file is NAM (Network Animator) file which is a visual display showing all the nodes and how packets flow takes place in a network scenario. They also provide trace files of the simulation that consists of the information about the packets that are transmitted, thus helps in performing post-analysis of the protocols.

For SAODV simulation, we use 50 nodes with 100 movement scenes with a maximum speed of 22ms with a simulation time period of 20 seconds to generate the scenario. At first, the network is created with multiple nodes which uses AODV protocol [3]. Its performance is evaluated using NAM files and trace files. The performance is evaluated in terms of security, network throughput and efficiency. Then an attacker node is implemented in AODV to create black hole attacked AODV protocol, it can be termed ad BAD-AODV. Perform the evaluation of BAD-AODV protocol. Now SAODV protocol is implemented which mitigates attacker nodes.

Now using gnu plot feature of the NS2 simulator, we compare the performance of the three protocols AODV, BAD-AODV and SAODV. We compare the security of protocols [5] using network packet loss rate. To compare the throughput, we use total data transmitted in a period of time in each protocols. The routing efficiency [6] is also taken into consideration for the comparison.

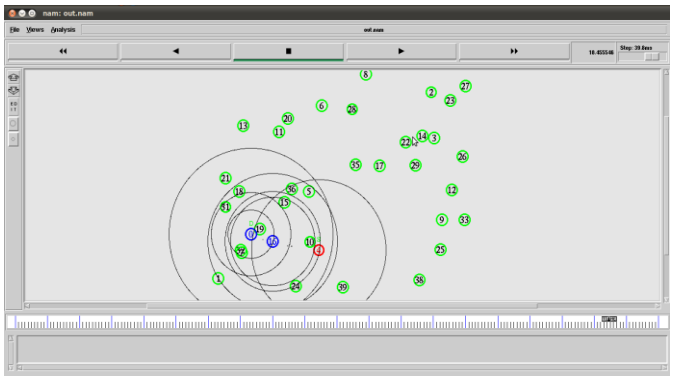

Figure 3: SAODV Protocol Implementation in NAM Animator of NS2 Simulator

TABLE 1
NETWORK PACKET LOSS RATE OF THE PROTOCOLS

| Protocols | Network Packet Loss Rate (%) |
|---|---|
| AODV | 8.13 |
| BAD-AODV | 57.7 |
| SAODV | 7.7 |

On comparing the network packet loss rate of the 3 protocols, as in table 1 and figure 4, we can see that the SAODV protocol with attacker nodes maintains low packet loss rate as that of AODV protocol without any attacker nodes.

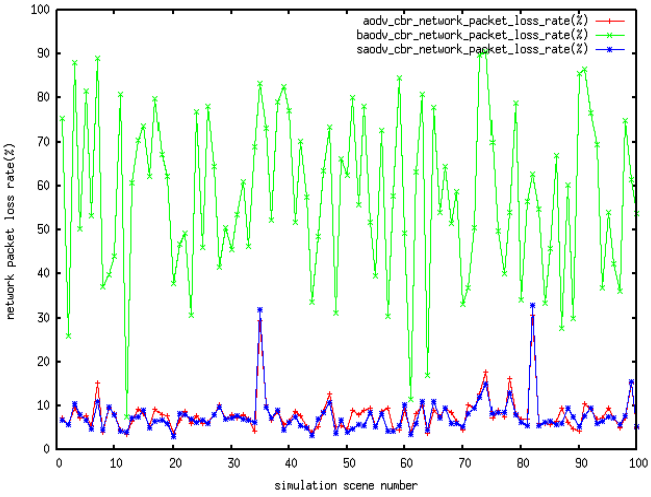


Figure 4: GNU plot of network packet loss rate comparison of the protocols

TABLE 2
NETWORK THROUGHPUT OF THE PROTOCOLS

| Protocols | Network Throughput (Mb/s) |
|---|---|
| AODV | 0.4755 |
| BAD-AODV | 0.213 |
| SAODV | 0.4758 |

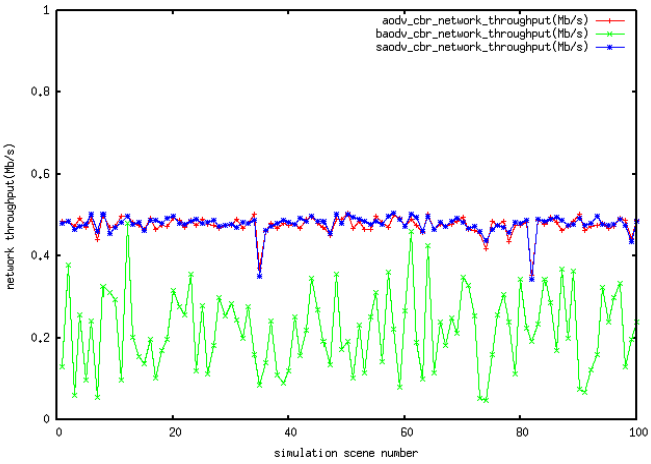


Figure 5: GNU plot of network throughput comparison of the protocols

When the network throughput of the protocols are compared in table 2 and figure 5, the SAODV protocol with a black hole has good throughput as better as that of AODV protocol without any black hole.

TABLE 3
NETWORK EFFICIENCY OF THE PROTOCOLS

| Protocols | Network Efficiency (%) |
|---|---|
| AODV | 39 |
| BAD-AODV | 23.77 |
| SAODV | 39.33 |

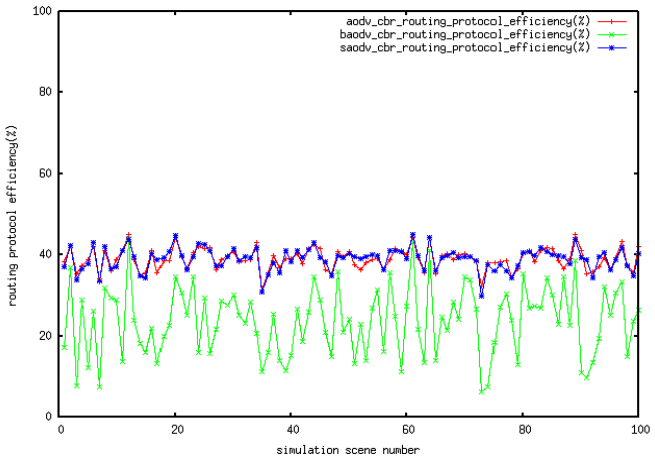


Figure 6: GNU plot of comparison of network efficiency of the protocols

As shown in table 3 and figure 6, we can understand that the SAODV protocol with malicious nodes maintains better network efficiency than that of AODV protocol without any malicious nodes.

## VII.EXPERIMENTAL RESULTS

As we can see in the experimental analysis, the SAODV protocol has better performance than the present AODV protocol in terms of network throughput, network efficiency and packet loss rate. SAODV protocol maintain a consistent performance and security even in the presence of a black hole or a malicious node.

The main benefits of using secure routing protocol SAODV are mainly: (i) They prevent the malicious node or the attacker node from getting the SSREP message so it won't be able to act as an intermediate node or destination node in the data transmission route, (ii) Even if the malicious node gets the SSREP message, it can arrive only later than the original one or the intercepted one because there is a time limit for the message to arrive at the destination which prevents the attacker node in delaying of message. It will eventually lead to detection of the black hole attack in the packet transmission scenario. (iii) In each and every route discovery process in the verification phase, the random number in the SRREP message packet is changed, so it will again reduce the probability of finding the SSREP by the attacker nodes.

## VIII. CONCLUSION & FUTURE WORKS

In the proposed paper, we can conclude that SAODV can effectively prevent black hole attack in VANET. They maintain a high routing efficiency. They ensure the security and privacy of the vehicles by not forwarding the routing packets without ensuring authenticity and integrity. So we can say that SAODV is an efficient protocol of vehicular network as they have a decent performance as well as security insurance.

In vehicles, there is a large number of wireless sensor nodes, in other terms, the embedded nodes. Since the automotive industry is shifting to electric era, they focus on battery power supply. So the embedded nodes require a good amount of power to work. The main source of energy consumption is the data transmission and reception between the wireless sensor nodes [8]. It must be dealt with high attention. So in case of SAODV, it requires more power for the computation that other protocols as they have an extra step called verification confirm phase.

Therefore, we need an improved SAODV routing protocol to reduce the power consumption of the embedded node by reducing the computational overhead in the communication processes. Our future works focus on the reduction of the computational overhead of the SAODV protocol without any compromise in the accuracy of detection of malicious nodes and black hole attacks in the VANET system.

## IX. REFERENCES


[1]. Ahmer Khan Jadoon, Licheng Wang, Tong Li, MuhammadAzam Zia "Lightweight Cryptographic Techniques for Automotive Cybersecurity", Hindawi Wireless Communications and Mobile Computing, Volume 2018, Article ID 1640167.

[2]. Dr.RamalingamSugumar, Jahir Hussain S, "The Enhanced Network Architecture, Route discovery and Data Transmission of AODV", International Journal of Pure and Applied Mathematics, Volume 116 No. 10 2017, 453-460

[3]. Mandeep Kaur Saggi Anshu Joshi, "EDMVP: Efficient Detection for Malicious Vehicles using AODV Protocol", Communications on Applied Electronics, Volume 2 – No.3, June 2015.

[4]. Anuja Thakur, Sharda Patel, Ashok Verma "Performance Evaluation of AODV, DSDV and DSR Routing Protocols using NS-2 Simulator", International Journal Of Engineering Sciences & Research Technology, Thakur, 3(1): January, 2014

[5]. Srivaths Ravi And Anand Raghunathan, Paul Kocher, Sunil Hattangady "Security In Embedded Systems: Design Challenges" ACM Transactions on Embedded Computing Systems, Vol. 3, No. 3, August 2004, Pages 461–491.

[6]. Madhu.B.M, Abhilash C B, "Implementation of Improved Robust Energy Efficient Routing Protocol", IEEE.978-1-4799-6629-5/14/$31.00_c 2014

[7]. Philipp Mundhenk, Andrew Paverd, Artur Mrowca, Sebastian Steinhorst, Martin Lukasiewycz, Suhaib A. FahmySamarjit Chakraborty, "Security In Automotive Networks: Lightweight Authentication And Authorization", ACM Transactions on Design Automation of Electronic Systems, Vol. 22, No. 2, Article 25, March 2017.

[8]. Jaspreet Singh, Er. Kartik Sharma, "A Review on Energy Efficient Routing In Mobile Ad-Hoc Networks (Manet)", IJESRT, Singh*, 4. (6): June, 2015].

[9]. Yugarshi Shashwat, Prashant Pandey, K. V. Arya &Smit Kumar, "A modified AODV protocol for preventing black hole attack in MANET". Information Security Journal, Pages 240-248, 25 Sep 2017.

[10]. Dr. Ajay N. Upadhyaya, Dr. J.S. Shah, "AODV Routing Protocol Implementation in VANET" International Journal of Advanced Research in Engineering and Technology, 10 (2), 2019, pp 585-595.

[11]. Rashmi Mishra, Akhilesh Singh, Rakesh Kumar, "VANET security: Issues, challenges and solutions", International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016.

[12]. Neeraj Varshney, Tumpa Roy, Niharika Chaudhary, "Security Protocol for VANET by Using Digital Certification to Provide Security with Low Bandwidth" International Conference on Communication and Signal Processing, April 3-5, 2014, India.

[13]. Muhammad Sameer Sheikh and Jun Liang, "A Comprehensive Survey on VANET Security Services in Traffic Management System", Hindawi Wireless Communications and Mobile Computing Volume 2019, Article ID 2423915.

[14]. Shivendra Prakash, Abhishek Swaroop, "A brief survey of blackhole detection and avoidance for ZRP protocol in MANETs", International Conference on Computing, Communication and Automation (ICCCA2016)

[15]. Mohamed Er-Rouidi, Houda Madini, Benachir El Hadadi, "Attacks against AODV Routing Protocol in Mobile Ad-Hoc Networks", 13th International Conference on Computer Graphics, Imaging and Visualization (CGiV), 2016



**Cite this article as :**

Angel Ann G Yesudasan, Tressa Michael, "SAODV Protocol Based Cryptographic Technique for Automotive Cybersecurity ", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 7 Issue 3, pp. 571-577, May-June 2020. Available at doi : https://doi.org/10.32628/IJSRSET207387
Journal URL : http://ijsrset.com/IJSRSET207387