Transmission Range Influence on Secure Routing in VANETs

Afef Slama
HANA Laboratory
University of Manouba
Manouba, Tunisia
e-mail: slama.afef@hotmail.fr

Ilhem Lengliz
Computer Science Department
Military Academy
Nabeul, Tunisia
e-mail: ilhem.lengliz@gmail.com

***Abstract*—With the rapid development in smart vehicles, the security and privacy issues of the Vehicular Ad-hoc Network (VANET) have drawn noteworthy regard. Indeed, every secure routing protocol must suit its operation to meet VANETs requirements and to yield a better security level. Incorporating Route Life Time (RLT) policy to Dynamic Source Routing (DSR) routing protocol is one of these adaptations. This policy intends to improve the global route lifetime. Trust Cryptographic Secure Routing (TCSR) protocol is one more proposition for secure routing found on the selection of the most trustworthy node all along with the route establishment. In this paper, we propose a comparative study of DSR-RLT and TCSR routing protocols on a highway to evaluate their performances in terms of transmission range variation. The simulation results show that TCSR exceeds DSR-RLT in terms of the packet loss ratio, average network throughput, and average delay.**

Keywords-VANET; secure routing; RLT; DSR-RLT; TCSR.

I. INTRODUCTION

VANETs refer to the Intelligent Transportation System (ITS) where vehicles are intelligent objects communicating (sending and receiving data) between each other in a smart manner [1]. Their purpose is to assist road users with appropriate services like safety, infotainment, and traffic management, by incorporating information and communication technology into vehicles and transport infrastructure. The transmission of messages in an open-access environment like VANETs leads to the most critical and challenging security issues [2]. As a result, the design of an effective secure routing protocol for VANET is crucial. So, the major threat is to design a robust and efficient secure routing algorithm that is very adaptable to frequent changes in the topology of fast-moving vehicles [3].

Diverse routing protocols have been proposed for VANETs to address the nodes' powerful mobility. Unfortunately, since most of these routing protocols use nodes succession during the route foundation among the source and the destination, the nature of communications characterized by a short duration may provide frequent disconnections. To handle this challenge, we provide in this work a comparison between two protocols we have proposed: the DSR-RLT protocol proposed in [4] and the TCSR protocol [5]. These protocols are found on the increase of the routing process's vigor toward regular common disconnections. The rest of this paper is organized as follows. Section II explores the DSR-RLT protocol. Section III gives a summary of the TCSR proposal. Section IV presents a comparison of the two protocols. The conclusion closes the article.

II. DSR-RLT

In an Intelligent Transportation System (ITS), each vehicle can be the sender, the receiver, or the router of every broadcasted message in the VANET. It is fundamental to secure the routing information since this information can be modified by malicious nodes. One of these secure routing protocols is DSR-RLT which is an enhancement of the native DSR routing protocol [6] using the Route Life Time (RLT) policy proposed in [7]. This policy seeks the optimal choice of the next hop based on the node's speed and the inter-node distances for a given approximation of the optimal number of hops in a VANET. When integrated into a routing operation, this policy tries to find an optimal choice of the next hop (relay node) in order to maximize the associated link lifetime and, hence, the overall route lifetime. Indeed, when invoked for a route building, the DSR-RLT protocol begins to look for the most favorable node positioning so as to cope with the RLT policy requirements such that the formed route for data transmissions will have the longest life time among all possible routes. In the same manner, the DSR-RLT protocol acts as the DSR protocol in establishing a route for a data packet to be sent on the VANET.

The preliminary evaluation of DSR-RLT protocol we carried out in [4] has shown that it achieves a higher network throughput in a realistic environment, especially on a crowded highway.

III. TCSR PROTOCOL

The trust metric has been proposed in various works addressing the secure routing in VANETs [8]-[10]. In this context, we have designed the Trust Cryptographic Secure Routing protocol (TCSR). Its operation takes place in two phases, as shown in Fig. 1 below. The first phase aims to create a high trust-surrounding level for each node in the VANET. It initiates calculating the trust level (TL_v) of each node in a dynamic and distributed model. Thereby, every vehicle is capable to assign a TL_v to every vehicle in its vicinity. Indeed, the evaluation of the behavior of a node is defined upon the interchanged packets. Therefore, depending

 ISBN: 978-1-61208-974-4

on the result of the overseeing process, the TL_v of each vehicle can rise, decline or stay fixed.

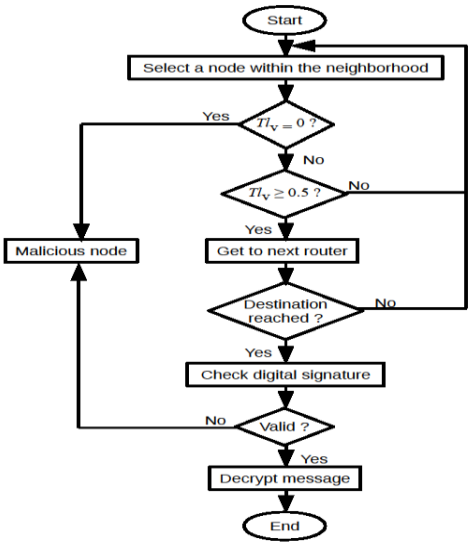

Figure 1. Flowchart of the TCSR operation process.

The second phase aims to enhance the security level of the TCSR model using asymmetric cryptography. Thus, the source information is ciphered using the public key of the sender to generate a digital signature. Therefore, the receiver authenticates the sender before decrypting the received message.

To compute the TL_v, the TCSR operation process is based on the reuse of the Additive Increase/Multicative-Decrease (AIMD) [11] technique along with the 3 DUP PKL (PacKet Losses) principle derived from the DUP ACK TCP congestion control mechanism. As illustrated in Fig. 2 below, at first, TCSR confesses that each vehicle in the transmission range (T_r) has a basic TL_0 in [0, 1] that may vary in time or over the routing process.

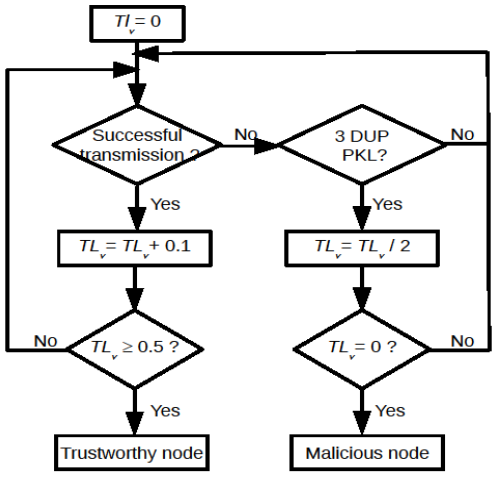

Figure 2. Flowchart of the node trust level monitoring.

The TCSR proposal allows each node to communicate with the others using a series of plausibility checks enabling them to compute the node score before selecting the one having the highest score. Consequently, the safest node is able to broadcast every signed message. In regard to RLT policy, it grants the choice of the route with the longest life time among all possible routes during the routing process of DSR-RLT.

IV. COMPARISON

It is interesting to evaluate the performances of the trust metric of the TCSR protocol on a highway and to compare its performances with those of DSR-RLT in order to verify the impact of the evolution on these two protocols.

A. Simulation model and parameters

For this study, we designed the VANETs scenario using Simulation of Urban Mobility (SUMO) [12]. We then converted the resulting SUMO trace file to be the data file used in NS-3.27. The objective of this simulation is to study the impact of the variation of the transmission range on a secure VANET routing protocol in order to evaluate its performance under different transmission ranges with variable data rates.

For the purpose of this study, we defined a VANET model with the parameters listed in Table 1 below. Two hundred nodes (vehicles) with a speed of 110 km/h were tested in the scenario to determine the impact of the network density on the TCSR and DSR-RLT secure routing process.

TABLE I. SIMULATION PARAMETERS OF A HIGHWAY

Parameter	Value
MAC layer	MAC IEEE 802.11p
Node buffer size	50 packets
Propagation model	Two Ray Ground
Network bandwidth	6 Mbps
Packet length	100, 200 & 512 Kb
Communication range	100 - 700 m
Highway length	6 km
Number of lanes	6 (3 in each direction)
Time of simulation	1800 sec

The performance indicators we selected to evaluate the two protocols in different VANETs scenarios are as follows: the Packet Loss Ratio (PLR), the average network throughput, the delay and the total energy consumed, which are the most relevant parameters commonly used to evaluate any given routing protocol in VANETs.

- Packet Loss Ratio (PLR): it is the loss rate of message delivery among vehicles within the same range of communication using single-hop messaging.

- Average Network Throughput: is the total payload over the entire session divided by the total time. Total time is calculated by taking the difference in timestamps between the first and last packet.
- Average Delay: it represents the period of time spent to route a packet from the source to the destination. That is the ratio of the number of sending bits in the packet to the throughput.
- Total Energy Consumed: it measures the total energy consumed by nodes during the routing process.

B. *Simulations results*

The purpose of this section is to examine the behavior of the TCSR and DSR-RLT protocols according to the variation of the transmission range and the traffic load.

Packet Loss Ratio (PLR): Fig. 3 describes the behavior of both protocols as a result of varying transmission range and transmitted packet size. We show that for a transmission range strictly less than or equal to 500 m, the value of PLR is inversely proportional to the value of the range for both protocols. It becomes proportional for a range strictly greater than 500 m, always for both protocols. This result is logical if we know that increasing the range of transmission with the maintenance of the number of vehicles reduces the number of jumps and thus ensures better connectivity that results in higher signal strength. On the other hand, when the transmission range exceeds 500 m, the conflict flow increases at the MAC layer resulting in a higher interference rate. Nevertheless, the CSMA/CA rules limit communication to many nodes avoiding collisions, which limit the reuse of bandwidth.

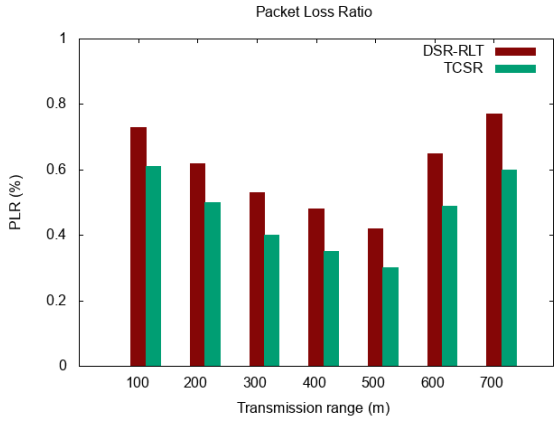

Figure 3. PLR vs Transmission range.

Fig. 3 shows the adaptability of the two protocols to more realistic road scenarios by adjusting the transmission range. However, it reveals better performance in terms of PLR for the TCSR protocol. This result is predictable because TCSR is essentially based on the value of the confidence level Tl_v of each vehicle. Thus, all relay nodes that it chooses during the routing process have the highest levels of trust. As a result, the number of internal attacks is reduced, which guarantees the successful transfer of the packets of the data signed by the CA to minimize external attacks. On a congested highway, TCSR differs from DSR-RLT in that it adjusts the confidence level of network nodes quickly with plausibility check series initiated. The longer the transmission range, the higher the number of vehicles traveling at high speeds, which increases the response time.

In addition, the lower performance of the DSR-RLT protocol is explained by the fact that the source routing keeps the complete path between the source and the destination in the header of the data packet. Besides, the use of the RLT policy which seeks the optimal choice of the next hop according to the speed of the node and the inter-node distances induces a loss of time during the phase of the construction of the road. The optimal choice of the relay node maximizes the lifetime of the link and therefore the overall life of the route but does not address the problem of internal and external attacks. As a result, the transmitted messages may be modified during the routing process which causes the loss of data.

Average Network Throughput: Fig. 4 shows the influence of the change in transmission range on the average network throughput following the deployment of the TCSR and DSR-RLT protocols. The PLR influences in the sense that the decrease of the PLR increases the flow. Thus, and as illustrated in Fig. 4, it increases for ranges less than or equal to 500 m and decreases for ranges strictly greater than 500 m.

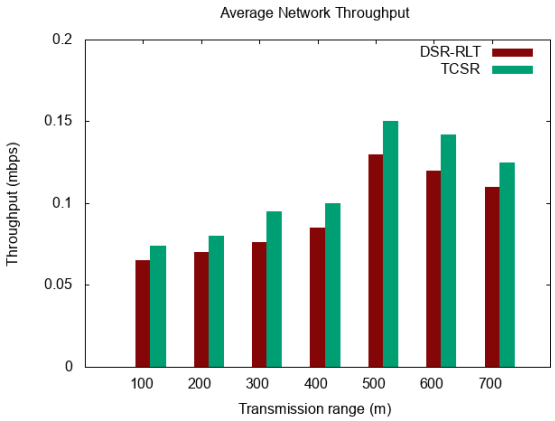

Figure 4. Average Network Throughput vs Transmission range.

We note that the average network throughput measured with the TCSR protocol decreases for the 600 m and 700 m transmission ranges, remains higher than the one provided by DSR-RLT. Indeed, the use of the AIMD mechanism for calculating the trust level of the relay nodes in addition to the digital signatures ensures better stability of the route during the routing of the data. It turns out that the detection of internal and external attacks throughout the routing increases network throughput.

Average Delay: Fig. 5 shows the behavior of both protocols as a result of varying transmission range and transmitted packet size. We show that for a transmission range strictly less than or equal to 500 m, the value of Average Delay is inversely proportional to the value of the range for both protocols. It becomes proportional for a range strictly greater than 500 m, always for both protocols. This

result is logical if we know that increasing the transmission range while maintaining the number of vehicles decreases the number of hops and thus guarantees greater connectivity that results in higher signal strength. On the other hand, when the transmission range exceeds 500 m, the conflict flow increases at the MAC layer resulting in a higher interference rate. Nevertheless, the CSMA/CA rules limit communication to many nodes avoiding collisions which limits the reuse of bandwidth.

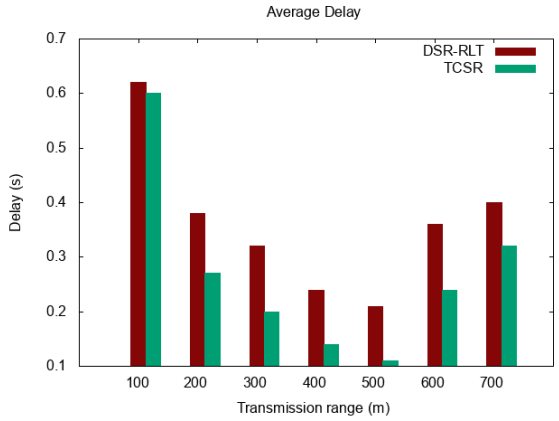

Figure 5. Average Delay vs Transmission range.

Fig. 5 shows the adaptability of the two protocols to more realistic road scenarios by adjusting the transmission range. However, it reveals better performance in terms of Average Delay for the TCSR protocol. This result is predictable because TCSR is fundamentally based on the value of the trust level Tl_v of each vehicle. Thus, all relay nodes that it chooses during the routing process have the highest levels of trust. As a result, the number of internal attacks is reduced, which guarantees the successful transfer of the packets of the data signed by the CA to minimize external attacks. On a congested highway, TCSR differs from DSR-RLT in that it adjusts the confidence level of network nodes quickly with plausibility check series initiated. The longer the transmission range, the higher the number of vehicles traveling at high speeds, which increases the response time.

In addition, the lower performance of the DSR-RLT protocol is explained by the fact that the source routing keeps the complete path between the source and the destination in the header of the data packet. Besides, the use of the RLT policy which seeks the optimal choice of the next hop according to the speed of the node and the inter-node distances induces a loss of time during the phase of the construction of the road. The optimal choice of the relay node maximizes the lifetime of the link and therefore the overall life of the route but does not address the problem of internal and external attacks. As a result, the transmitted messages may be modified during the routing process which causes the loss of data.

Total Consumed Energy: Fig. 6 shows the influence of the change in transmission range on the amount of Total Consumed Energy following deployment of the TCSR and DSR-RLT protocols. Thus, and as illustrated in Fig. 6, TCSR has the uppermost amount of consumed energy which is also expected since the RLT policy reduces the number of control packets generated to establish a route between a source and a destination. While the TCSR employs a trust metric and a cryptography strategy known for their complexity. But we should recall that this may not affect the network overall status given that vehicles in VANETs are equipped with OBUs and batteries.

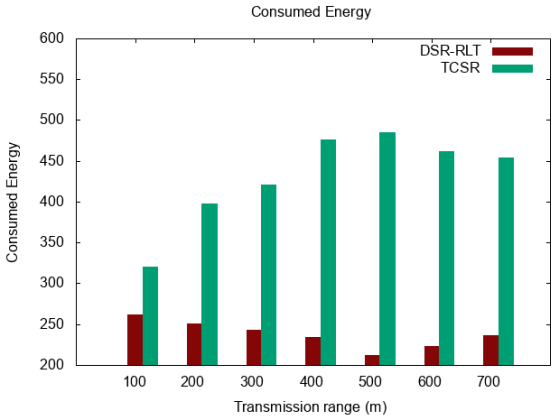

Figure 6. Total Consumed Energy vs Transmission range.

The TCSR protocol is suitable for managing a fast and continuous network topology. Indeed, this protocol makes it possible to deliver more packet than the protocol DSR-RLT, it also reaches better performances in term of flow for a T_r equal to 500 m.

V. CONCLUSION

In this paper, we presented a comparison between the TCSR protocol that uses the trust metric and the DSR-RLT protocol based on RLT policy. We chose to compare their respective performances on a congested highway for different transmission ranges. We found that the TCSR protocol is better adapted to scalability due to its performance in terms of PLR, average network throughput and average delay for transmission range values up to 500 m. However, it indicates a poor effect in terms of consumed energy compared to DSR-RLT for all transmission ranges. For transmission range values strictly greater than 500 m, a study should be developed based on the variation of simulation parameters such as bandwidth and data packet size.

REFERENCES

[1] F. Cunha, L.Villas, A. Boukerche, G. Maia, A. Viana, R.A.F. Mini, and A.A.F. Loureiro, “Data communication in vanets: survey, applications and challenges”, Ad Hoc Networks journal, vol. 44, pp 90 - 103, 2016.

[2] S. S. Manvi and S. Tangade, “A survey on authentication schemes in VANETs for secured communication”, Vehicular Communications, vol. 9, pp. 19-30, July 2017.

[3] Y. Hammouche and S. Merniz, “Vanet cross layer routing”, 2019 International Conference of Computer Science and Renewable Energies (ICCSRE), July 2019.

[4] I. Lengliz and A. Slama, “ Enhancing VANETs' Routing Operation with the Route Lifetime Policy”, International

Journal of Computer Applications, vol. 164, pp. 35-40, April 2017.

[5] A. Slama, I. Lengliz and A. Belghith, "TCSR: an AIMD Trust-based Protocol for Secure Routing in VANET", The 2018 International Conference on Smart Applications, Communications and Networking, November 2018.

[6] D. Johnson, Y. Hu, D. Maltz, RFC 4728, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4", February 2007.

[7] D. Kumar, A. A. Kherani, E. Altman. "Route Life time based Interactive Routing in Intervehicle Mobile Ad Hoc Networks", Research Report, INRIA, France, September 2005.

[8] T. Gazdar, A. Rachedi, A. Benslimane, and A. Belghith, "A distributed advanced analytical trust model for vanets", 2012 IEEE Global Communications Conference (GLOBECOM), December 2012.

[9] A. Chinnasamy, S.Prakash and P.Selvakumari, "Enhance trust based routing techniques against sinkhole attack in AODV based VANET", International Journal of Computer Applications, vol. 65, issue 15, March 2013.

[10] T. Gazdar, A. Belghith, and H. Abutar, "An Enhanced and Distributed Trust Computing Protocol for VANETs", IEEE Access, vol. 6, pp. 380-392, October 2017.

[11] RFC5681, TCP Congestion Control.

[12] http://sumo.sourceforge.net. Accessed April 2022.

 ISBN: 978-1-61208-974-4