Security Analysis and Improvement of Lightweight VANET Authentication Protocol (Case Study : Zhao et al. LVAP)

Septha Siswantyo¹⁾

¹⁾ Politeknik Siber dan Sandi Negara, Indonesia

¹⁾ sepha.siswantyo@poltekssn.ac.id

ABSTRACT

VANET is an ad-hoc network implemented on vehicle communication to ensure traffic safety and traffic management efficiency. VANET security is a concern because of various vulnerabilities, especially from authentication criteria that the attacker can exploit. VANET is vulnerable to Sybil attack, entity impersonation, message modification, and identity falsification. Several mechanisms and protocols have been developed to address these vulnerabilities. The design of the VANET authentication protocol also needs to be proven using formal methods to ensure that the protocol meets the required security criteria. In this research, the security of VANET authentication protocol developed by Zhao et al. was analyzed using the Datta et al. security protocol analysis method. Instead of BAN Logic, the Scyther tool was used to verify security claims and find possible attacks. Our Security analysis results show that Zhao et al.'s protocol does not meet confidentiality and entity authentication criteria. Scyther tool can find attacks on nonce confidentiality and man-in-the-middle attack. Therefore, we modify Zhao et al. protocol by adding signature and session key confirmation to improve its security. Based on analysis results, our modified Zhao et al. authentication protocol met confidentiality and entity authentication criteria. The use of signature and session key confirmation prevents man-in-the-middle attack and protects nonce confidentiality. Therefore, our research concludes that modified Zhao et al. authentication protocol more secure than the original protocol in terms of nonce and session key confidentiality, aliveness, weak agreement, non-injective agreement, and non-injective synchronization.

Keywords: VANET; authentication; formal methods; Scyther; confidentiality, man-in-the-middle

INTRODUCTION

Vehicular ad hoc network (VANET) combines wireless communication with data sharing capabilities on vehicles to connect to the network and provide or use network services such as use in offices and residences (Rasheed et al., 2017). The primary purpose of implementing VANET is to provide information related to traffic safety and improve traffic management efficiency (Abdellah et al., 2019). VANET has several characteristics, including high mobility, dynamic network topology, depending on computing and storage capabilities, time criticality, and limited transmission power (Sheikh & Liang, 2019). Security is one of the crucial aspects of VANET implementation. VANET is vulnerable to attack because of its unique characteristics. Therefore, VANET must meet several security criteria, including confidentiality, data integrity, availability, authentication, non-denial, privacy and anonymity, access control, data verification, traceability, and the ability to revoke identity (Hasrouny et al., 2017). Authentication in VANET plays a very vital role, especially authentication of entities and messages. Some of the attacks that exploit weaknesses in VANET include Sybil attacks, impersonation of actual entities (acting like entities), replay attacks, key and certificate replication, message modification, and masquerade attacks (identity forgeries) (Sheikh & Liang, 2019).

Several cryptographic protocols have been developed for authentication on VANET. Some protocol designed with formal analysis to prove its security. Liu et al. lightweight VANET authentication protocol (LVAP) and Zhao et al. LVAP used BAN Logic as manual formal analysis tool (Liu et al., 2017; Zhao et al., 2018). while NERA and LPPA used the game theory tool (Bayat et al., 2020; Zhou et al., 2020). Combination of manual and automated method also can be used to analyze designed protocol. NECPPA protocol analyzed with game theory and Proferif (Pournaghi et al., 2018). BAN Logic and AVISPA used to analyze SAPSC protocol (Kanchan et al., 2019). AVISPA also used to

* Corresponding author

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NoDerivatives 4.0 International License.

analyze RSEAP protocol, combined with game theory method (Kumar et al., 2020). One of the methods mentioned above, BAN Logic, has some weaknesses, such as lack of assumptions, message, and different protocol runs considerations, and subjectivity problem (Agustina et al., 2019; Patel et al., 2010). In this research, we analyze the security criteria of Zhao et al. LVAP with Datta et al. methodology and Scyther tool. We analyze Zhao et al. LVAP with new tool to find protocol vulnerabilities and possible attacks that BAN Logic cannot find. We also propose a modification of Zhao et al. protocol based on security analysis finding from the original protocol and prove that the modified protocol fulfilled security criteria for VANET authentication protocol.

LITERATURE REVIEW

The development of authentication protocol of VANET has been published and offers many different mechanisms to secure VANET communication. In 2017, Liu et al. lightweight V2I authentication protocol using secret sharing method and analyze with BAN Logic (Liu et al., 2017). Liu et al. LVAP achieve message authentication, confidentiality, and practical anonymity. Zhao et al. also propose a lightweight authentication protocol for VANET based on public key. This protocol was analyzed with BAN Logic and achieve authentication goal. Zhao et al. also claim that the designed LVAP resist password guessing attack, man-in-the-middle (MITM) attack, and replay attack. Bayat et al. develop NERA protocol that embeds master key in tamper-proof device (TPD) at roadside infrastructure unit (RSU) (Bayat et al., 2020). Formal analysis based on game theory conducted to NERA and prove that NERA achieves message integrity, authentication, and identity privacy. Game theory-based analysis is also used to analyze LPPA protocol (Zhou et al., 2020). LPPA was designed as a lightweight authentication protocol for location-based services in VANET. LPPA claimed achieves vehicle location privacy, interest and interest pattern privacy. Pournaghi et al. also integrate TPD and RSU scheme to design NECPPA protocol (Pournaghi et al., 2018). NECPPA combines Proverif and game theory methods for formal analysis. Proverif proves that NECPPA achieves authentication and observational equivalence, while game theory method proves achievement of message integrity and authentication and identity privacy. Another combination is BAN Logic and AVISPA, which are used to analyze SAPSC protocol (Kanchan et al., 2019). SAPSC protocol implements signcryption mechanism to secure VANET group communication. Formal analysis of SAPSC shows that secrecy and mutual authentication are fulfilled. Kumar et al., in 2020, proposed RSEAP, an authentication protocol based on RFID (Kumar et al., 2020). RSEAP analyzed with game theory and AVISPA and gave the result that RSEAP secure against MITM and replay attack. Scyther tool that we used in this research was also used to analyze RSEAP2, an improvement of RSEAP. Scyther's result shows that RSEAP2 satisfies confidentiality and authentication (Safkhani et al., 2021).

METHOD

The method used in this research is security protocol analysis method consisting of protocol and attacker modeling, specifying security criteria, and checking or proving security criteria (Datta et al., 2010). We use Scyther tool for checking security criteria. Scyther is an automated security protocol verification tool developed based on symbolic model (Cremers, 2014). Scyther takes security protocol model that includes security claims as input and evaluates these. Zhao et al. LVAP consists of a three-way authentication message between vehicle client C as vehicle security gateway and cloud server S as VANET infrastructure. The protocol step is as follow:

Message 1 $C \rightarrow S : \{C, N_c\}_{PK_S}$
Message 2 $S \rightarrow C : \{N_c, N_s, K_{cs}\}_{PK_C}$
Message 3 $C \rightarrow S : N_s$

Zhao et al. LVAP steps are modeled with Security Protocol Description Language (SPDL). Table 1 shows protocol model in Scyther.

In this research, the attacker is modeled under the Dolev-Yao model. Dolev-Yao model is integrated with Scyther tools by default. In the Dolev-Yao attacker model, an attacker can intercept all communications on the network, initiate a connection, and send data to other entities on the network. This capability allows attackers to act as man-in-the-middle (MITM) (Do et al., 2019).

After modeling the protocol and attacker, the next step is specifying security criteria. The security criteria of the protocol to be verified include confidentiality and entity authentication. "Secret" claim syntax indicates criteria for the confidentiality of nonce N_c and N_s and the confidentiality of the session key K_{cs} for each role. Meanwhile, entity

authentication criteria are verified based on different authentication levels, such as “Alive” (aliveness), “Weakagree” (weak agreement), “Niagree” (non-injective agreement), and “Nisynch” (non-injective synchronization). Complete explanation of the differences in each authentication level can be seen in (Lauser et al., 2020) and (Cremers & Mauw, 2012).

Table 1
Zhao et al. LVAP Protocol Model

Protocol Model	
#Light_VANET	role S{
usertype SessionKey;	fresh Ns: Nonce;
protocol lightvanet(C,S){	fresh Kcs: SessionKey;
role C{	var Nc: Nonce;
fresh Nc: Nonce;	
var Ns: Nonce;	recv_1(C,S, {C,Nc}pk(S));
var Kcs: SessionKey;	send_2(S,C, {Nc,Ns,Kcs}pk(C));
	recv_3(C,S, Ns);
send_1(C,S, {C,Nc}pk(S));	
recv_2(S,C, {Nc,Ns,Kcs}pk(C));	claim_S1(S,Secret,Nc);
send_3(C,S, Ns);	claim_S2(S,Secret,Nc);
	claim_S3(S,Secret,Kcs);
claim_C1(C,Secret,Nc);	claim_S4(S,Alive);
claim_C2(C,Secret,Ns);	claim_S5(S,Weakagree);
claim_C3(C,Secret,Kcs);	claim_S6(S,Niagree);
claim_C4(C,Alive);	claim_S7(S,Nisynch); }}
claim_C5(C,Weakagree);	
claim_C6(C,Niagree);	
claim_C7(C,Nisynch); }	

The next stage of security protocol analysis method is checking or proving the security criteria using the Scyther verification tool. Before doing the verification, Scyther first checked the protocol modeling based on the syntax and message order. Scyther then verifies the security criteria based on the claims already included in the modeling. Scyther have command-line tool and graphical user interface (GUI) tool. GUI tool adds usability features and interact with command-line tool automatically as the backend. Figure 1 shows how GUI tool works and interacts with command-line tool. We use GUI tool of Scyther in this research to directly check patterns from each claim if an attack exists. In the background process, Scyther uses semantic analysis to check all possibilities of iterations and find possible attacks on protocol with heuristic method. If one of the claims is met, an "OK" statement will appear in the status column in the same row. If the claim is not fulfilled, a "FAIL" statement will appear, and the option to display an attack graph will be available.

Fig. 1 Scyther GUI and Command-line Interaction (Alharbi et al., 2015)

RESULT

Security criteria checking was conducted by verifying protocol model on Scyther. The verification results as shown in Figure 2 show several failed or unfulfilled claims from both roles. On the *C* side, one claim failed out of seven claims. While on the *R* side, five claims were failed. For each failed claim, there must be at least one attack.

Claim	Status	Comments	Pattern
lightvanet.C1 Secret N_c	OK	Verified	No attacks.
lightvanet.C2 Secret N_s	Fail	Falsified	At least 1 attack. 1 attack
lightvanet.C3 Secret K_{cs}	OK	Verified	No attacks.
lightvanet.C4 Alive	OK	Verified	No attacks.
lightvanet.C5 Weakagree	OK	Verified	No attacks.
lightvanet.C6 Niagree	OK	Verified	No attacks.
lightvanet.C7 Nisynch	OK	Verified	No attacks.
lightvanet.S1 Secret N_c	Fail	Falsified	At least 1 attack. 1 attack
lightvanet.S2 Secret N_s	Fail	Falsified	At least 1 attack. 1 attack
lightvanet.S3 Secret K_{cs}	OK	Verified	No attacks.
lightvanet.S4 Alive	OK	Verified	No attacks.
lightvanet.S5 Weakagree	Fail	Falsified	At least 1 attack. 1 attack
lightvanet.S6 Niagree	Fail	Falsified	At least 1 attack. 1 attack
lightvanet.S7 Nisynch	Fail	Falsified	At least 1 attack. 1 attack

Fig. 2 Zhao et al. LVAP Verification Results

Fig. 3 Attacks on C2 Secret N_s Claim

Fig. 4 Attacks on S1 Secret N_c Claim

Verification of the N_s confidentiality claim on role C ($C2$ Secret N_s) results in one attack, as shown in Figure 3. Nonce N_s value can be directly obtained by the attacker when intercepting Message-3 from C because N_s value is not encrypted. Figure 4 shows the attack graph on N_c confidentiality (from $S1$ Secret N_c claim). The attacker (Eve) can impersonate server S . Client C assume communicating with legitimate S . Then, C creates Message-1 by encrypting identity C and nonce N_c with the attacker's public key. The attacker receives and decrypts Message-1 with his private key and obtains the nonce N_c . Figure 5 shows results of the verification of claim $S2$ Secret N_s . The attacker can impersonate S and receive the unencrypted nonce N_s directly. Based on the Dolev-Yao model, the attacker can also immediately find out the contents of the Message-3 sent in plaintext because it can intercept every message from each entity.

Three authentication claims, namely ($S5$ Weakagree), ($S6$ Niagree), and ($S7$ Nisynch), were not fulfilled. The verification results of the three claims also produce the same attack graph, as can be seen in Figure 6. The "Weakagree" claim is not fulfilled because when S completes the protocol (on $recv_3$), it does not communicate with the original S in the previous message sequence, specifically when sending Message-1 ($send_1$) and receives Message-2 ($recv_2$). The attacker can impersonate S to receive Message-1 and send Message-2 to C . So C does not communicate with the real S even though S has completed a protocol session. The claims of "Niagree" and "Nisynch" are also not fulfilled because both claims require the same basic conditions as "Weakagree".

Fig. 5 Attacks on $S2$ Secret N_s Claim

Fig. 6 Attacks on $S5$ Weakagree Claim

We propose a protocol modification to improve Zhao et al.'s protocol security. Modifications are made by adding a digital signature mechanism in second message and encryption to the last message as key confirmation. The modified protocol step is as follow:

Message 1 $C \rightarrow S : \{C, N_c\}_{PK_S}$

Message 2 $S \rightarrow C : \{N_c, N_s, K_{cs}, \{N_c, N_s, K_{cs}\}_{PK_S}\}_{PK_C}$

Message 3 $C \rightarrow S : \{N_s\}_{K_{cs}}$

Table 2 shows modified protocol model in Scyther. We also analyze the security of modified protocol using the same method with some changes in protocol model. The attacker model and security criteria to be verified still the same as used in previous original protocol analysis.

Table 2
Modified Zhao et al. LVAP Protocol Model

Protocol Model	
#Modified_Light_VANET	role S {
usertype SessionKey;	fresh Ns: Nonce;
protocol lightvanet(C,S){	fresh Kcs: SessionKey;
role C {	var Nc: Nonce;
fresh Nc: Nonce;	
var Ns: Nonce;	recv_1(C,S, {C,Nc}pk(S));
var Kcs: SessionKey;	send_2(S,C, {Nc,Ns,Kcs, {Nc,Ns,Kcs}sk(S)}pk(C));
	recv_3(C,S, {Ns}Kcs);
send_1(C,S, {C,Nc}pk(S));	
recv_2(S,C, {Nc,Ns,Kcs, {Nc,Ns,Kcs}sk(S)}pk(C));	claim_S1(S,Secret,Nc);
send_3(C,S, {Ns}Kcs);	claim_S2(S,Secret,Nc);
	claim_S3(S,Secret,Kcs);
claim_C1(C,Secret,Nc);	claim_S4(S,Alive);
claim_C2(C,Secret,Ns);	claim_S5(S,Weakagree);
claim_C3(C,Secret,Kcs);	claim_S6(S,Niagree);
claim_C4(C,Alive);	claim_S7(S,Nisynch); }
claim_C5(C,Weakagree);	
claim_C6(C,Niagree);	
claim_C7(C,Nisynch); }	

The results of the verification of the modified VANET Zhao et al. authentication protocol are shown in Figure 7.

Claim	Status	Comme
modifiedlightvanet.C	Ok	Verified
modifiedlightvanet.C1	Ok	Verified
modifiedlightvanet.C2	Ok	Verified
modifiedlightvanet.C3	Ok	Verified
modifiedlightvanet.C4	Ok	Verified
modifiedlightvanet.C5	Ok	Verified
modifiedlightvanet.C6	Ok	Verified
modifiedlightvanet.C7	Ok	Verified
modifiedlightvanet.S1	Ok	Verified
modifiedlightvanet.S2	Ok	Verified
modifiedlightvanet.S3	Ok	Verified
modifiedlightvanet.S4	Ok	Verified
modifiedlightvanet.S5	Ok	Verified
modifiedlightvanet.S6	Ok	Verified
modifiedlightvanet.S7	Ok	Verified

Fig. 7 Modified Zhao et al. LVAP Verification Results

DISCUSSIONS

Based on the results from Scyther, five security criteria are failed to achieve for original Zhao et al. LVAP. Zhao et al. LVAP also vulnerable to MITM attack. This is contradiction with security claimed by Zhao et al. We propose modification of Zhao et al. protocol and analyze with Scyther. Based on the results, all security claims were successfully fulfilled, and no attacks were found from our proposed protocol. Our implementation of signature and key confirmation improve security of Zhao et al. protocol. The attacker is assumed to be unable to compute an entity's private key even though the public key is known in Dolev-Yao model. The attacker cannot impersonate S completely because he must also know the private key value of S to continue the communication (as a man-in-the-middle). Suppose the attacker is still trying to use a fake private key and create Message-2 with his signature. In that case, C will detect message forgery if there is a difference between the digital signature value of the calculated N_c parameter and that received from S . The authenticity of N_c sent back by S is guaranteed through a digital signature. This condition leads to the following successful security claim.

Table 3
Comparison of Security Claim

Security claim	Zhao et al. LVAP	
	Original	Modified
N_c Confidentiality	×	√
N_s Confidentiality	×	√
K_{cs} Confidentiality	√	√
Aliveness	√	√
Weak Agreement	×	√
Ni-Agreement	×	√
Ni-Synchronization	×	√

Note: √ (achieved), ×(not achieved)

The attacker cannot obtain N_c by decrypting Message-1 because he unable to impersonate S and get involved in the following message. N_s confidentiality is also maintained through the encryption mechanism performed by C on Message-3 using the session key. The message can only be opened by the original S whose generated the session key previously. Weakagree's claim is fulfilled on S 's side because S completed a session with C , who also previously communicated with the original S . Niagree's claim is fulfilled because when S completed a session with C , who had also previously communicated with the original S , the data exchanged, i.e., N_s and N_c , correspond and do not change. Nisynch's claim is fulfilled because when S completed a session with C , who also previously communicated with the original S , then the data exchanged (N_s and N_c) matched and did not change, and according to the order of messages

that should be. Additionally, Message-3 also serves as a session key confirmation to ensure that C and S already have the same session key to encrypt the following communication session. Table 3 shows comparison of security claim achieved between original and modified Zhao et al. LVAP. However, our security claims comparison limited to properties defined by Scyther. Scyther can not verify injective agreement and injective synchronization, which leads to security against replay attacks.

CONCLUSION

Based on security analysis with the Datta et al. method and Scyther tool, Zhao et al. LVAP does not meet the confidentiality and authentication criteria. However, our modification with signature and session key confirmation gives improvements to the original protocol security. Furthermore, Scyther results show that our modified Zhao et al. LVAP achieve confidentiality and authentication criteria.

REFERENCES

- Abdellah, A. R., Muthanna, A., & Koucheryavy, A. (2019). Robust Estimation of VANET Performance-Based Robust Neural Networks Learning. In O. Galinina, S. Andreev, S. Balandin, & Y. Koucheryavy (Eds.), *Internet of Things, Smart Spaces, and Next Generation Networks and Systems* (Vol. 11660, pp. 402–414). Springer International Publishing. https://doi.org/10.1007/978-3-030-30859-9_34
- Agustina, E. R., Christine, M., & Fitriani, I. (2019). Analisis Protokol CryptO-ON2 dengan Menggunakan Scyther Tool. *Jurnal Teknologi Informasi dan Ilmu Komputer*, 6(1), 107. <https://doi.org/10.25126/jtiik.2019611303>
- Alharbi, E., Alsulami, N., & Batarfi, O. (2015). An Enhanced Dragonfly Key Exchange Protocol against Offline Dictionary Attack. *Journal of Information Security*, 06(02), 69–81. <https://doi.org/10.4236/jis.2015.62008>
- Bayat, M., Pournaghi, M., Rahimi, M., & Barmshoory, M. (2020). NERA: A new and efficient RSU based authentication scheme for VANETs. *Wireless Networks*, 26(5), 3083–3098. <https://doi.org/10.1007/s11276-019-02039-x>
- Cremers, C. (2014). *Scyther User Manual*. <https://github.com/cascremers/scyther/blob/master/gui/scyther-manual.pdf>
- Cremers, C., & Mauw, S. (2012). *Operational Semantics and Verification of Security Protocols*. Springer Berlin Heidelberg. <http://link.springer.com/10.1007/978-3-540-78636-8>
- Datta, A., Jha, S., Li, N., Melski, D., & Reps, T. (2010). Analysis Techniques for Information Security. *Synthesis Lectures on Information Security, Privacy, and Trust*, 2(1), 1–164. <https://doi.org/10.2200/S00260ED1V01Y201003SPT002>
- Do, Q., Martini, B., & Choo, K.-K. R. (2019). The role of the adversary model in applied security research. *Computers & Security*, 81, 156–181. <https://doi.org/10.1016/j.cose.2018.12.002>
- Hasrouny, H., Samhat, A. E., Bassil, C., & Laouti, A. (2017). VANet security challenges and solutions: A survey. *Vehicular Communications*, 7, 7–20. <https://doi.org/10.1016/j.vehcom.2017.01.002>
- Kanchan, S., Singh, G., & Chaudhari, N. S. (2019). SAPSC: SignReencrypting authentication protocol using shareable clouds in VANET groups. *IET Intelligent Transport Systems*, 13(9), 1447–1460. <https://doi.org/10.1049/iet-its.2018.5474>
- Kumar, V., Ahmad, M., Mishra, D., Kumari, S., & Khan, M. K. (2020). RSEAP: RFID based secure and efficient authentication protocol for vehicular cloud computing. *Vehicular Communications*, 22, 100213. <https://doi.org/10.1016/j.vehcom.2019.100213>
- Lauser, T., Zelle, D., & Krauß, C. (2020). Security Analysis of Automotive Protocols. *Computer Science in Cars Symposium*, 1–12. <https://doi.org/10.1145/3385958.3430482>
- Liu, Y., Guo, W., Zhong, Q., & Yao, G. (2017). LVAP: Lightweight V2I authentication protocol using group communication in VANETs. *International Journal of Communication Systems*, 30(16), e3317. <https://doi.org/10.1002/dac.3317>
- Patel, R., Borisaniya, B., Patel, A., Patel, D., Rajarajan, M., & Zisman, A. (2010). Comparative Analysis of Formal Model Checking Tools for Security Protocol Verification. In N. Meghanathan, S. Boumerdassi, N. Chaki, & D. Nagamalai (Eds.), *Recent Trends in Network Security and Applications* (Vol. 89, pp. 152–163). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-14478-3_16

-
- Pournaghi, S. M., Zahednejad, B., Bayat, M., & Farjami, Y. (2018). NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET. *Computer Networks*, 134, 78–92. <https://doi.org/10.1016/j.comnet.2018.01.015>
- Rasheed, A., Gillani, S., Ajmal, S., & Qayyum, A. (2017). Vehicular Ad Hoc Network (VANET): A Survey, Challenges, and Applications. In A. Laouiti, A. Qayyum, & M. N. Mohamad Saad (Eds.), *Vehicular Ad-Hoc Networks for Smart Cities* (Vol. 548, pp. 39–51). Springer Singapore. https://doi.org/10.1007/978-981-10-3503-6_4
- Safkhani, M., Camara, C., Peris-Lopez, P., & Bagheri, N. (2021). RSEAP2: An enhanced version of RSEAP, an RFID based authentication protocol for vehicular cloud computing. *Vehicular Communications*, 28, 100311. <https://doi.org/10.1016/j.vehcom.2020.100311>
- Sheikh, M. S., & Liang, J. (2019). A Comprehensive Survey on VANET Security Services in Traffic Management System. *Wireless Communications and Mobile Computing*, 2019, 1–23. <https://doi.org/10.1155/2019/2423915>
- Zhao, G., Wang, R., Wang, X., & Zhu, X. (2018). Design and Formal Verification of a VANET Lightweight Authentication Protocol. *2018 IEEE 18th International Conference on Communication Technology (ICCT)*, 513–517. <https://doi.org/10.1109/ICCT.2018.8600064>
- Zhou, J., Cao, Z., Qin, Z., Dong, X., & Ren, K. (2020). LPPA: Lightweight Privacy-Preserving Authentication From Efficient Multi-Key Secure Outsourced Computation for Location-Based Services in VANETs. *IEEE Transactions on Information Forensics and Security*, 15, 420–434. <https://doi.org/10.1109/TIFS.2019.2923156>