ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 2, February 2020

A Review and Challenges of Security Issue over V2V Ad-Hoc Communication

Madhu Mala[1], Prof. Nitesh Kumar[2], Prof. Keshav Mishra[3]

M.Tech Scholar, Department of Electronics and Communication, Sagar Institute of Research Technology & Science, Bhopal, India[1]

Assistant Professor, Department of Electronics and Communication, Sagar Institute of Research Technology & Science, Bhopal, India[2]

Associate Professor, Department of Electronics and Communication, Sagar Institute of Research Technology & Science, Bhopal, India[3]

ABSTRACT: VANETs have been appeared as a new area of data dissemination process in which vehicles provide aid to the end users. Vehicles in vehicular ad hoc network have highly unstable (dynamic) topology which produces hindrances in timely delivery of sensitive messages Vehicular Ad-hoc networks (VANETs) are very likely to be deployed in the coming years because of the safety requirements and thus become the most relevant form of mobile ad hoc networks. Security is the main issue in VANETs because of the main use of the VANETs is for safety related application and in that case the viability of the security may cause harm to human lives. In this paper, we address the security issues of these networks and its consequences overhead in VANETs.

KEYWORDS: Cascade, Cryptography, Multiple, Vehicular Ad-hoc Networks.

I. INTRODUCTION

VANET is a type of mobile ad hoc network (MANET) with road routes, which aim to provide traffic safety, improve traffic flow, and enhance the driving experiences. It relies on transportation authorities for registering and managing the roadside units (RSUs) and onboard units (OBUs). An OBU is installed in every vehicle as a transmitter to communicate with other vehicles on the road, while RSUs are installed along the street with network devices. RSUs are used to communicate with the infrastructure and contain network devices for dedicated short-range communication (DSRC). VANETs are classified into two categories: vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications [6]. In the V2V, vehicles can communicate with each other in order to exchange traffic-related information. In the V2I, vehicles can directly communicate with the infrastructure to exchange traffic information. In recent years, significant development and advances in vehicular technology have provide many resources such as storage devices, radio network, robust computational power, and different kinds of vehicle sensors.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 2, February 2020

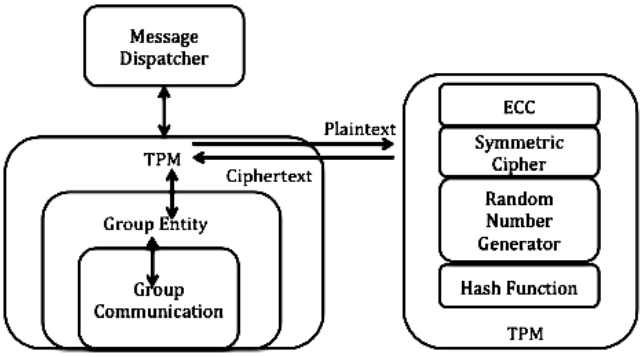

Figure 1: Trust Grouping Framework and TPM architecture

Wireless sensor networks (WSNs) are the robust technology for the Internet of Things (IoT) and significantly applied in ITS. In this technology, sensors are fixed on the roadside to identify the traffic situations and deliver the traffic-related information to vehicles such as collision warning, lane-changing warning, and more. This traffic information can significantly enhance the traffic and road safety and improve driving experiences. In the ITS context, WSNs can be regarded as an additional element in which they can cooperate with the vehicular network, i.e., VANETs. This integration between vehicular ad hoc and wireless sensor networks forms a hybrid network, termed VANET-WSN.

Intelligent connected vehicles are autonomous vehicles. With the increasing degree of automation of autonomous vehicles and the development of open applications in the future, the computing tasks of autonomous vehicles are becoming more and more complex. In practice, the computing resources of vehicles are limited and the processing of data is not always guaranteed to be completed in time. However, the timely processing and integrity of the data are very important for vehicles because it affects the path selection of the traveling vehicle and the passenger experience. Therefore, it is necessary to reduce latency in processing data and verify the integrity of data for vehicles.

II. RELATED WORK

Y. Yang et al.,[1] It is study the periods of sequences produced by the cascade connection of two Feedback shift registers (FSRs). The period of the cascade connection is the period of the longest sequences it produces. An upper bound for the period of the cascade connection of a nonlinear feedback shift register (NFSR) into a Linear feedback shift register (LFSR) is established. In addition, the cascade connection of an n -stage maximum-length LFSR into an n-stage NFSR is called an (n + n)-stage Grain-like NFSR, and it is propose two families of (n + n)stage Grain-like NFSRs such that the minimal period 2 n - 1 is achievable for a positive integer.

H. Zhong et al., [2] In this work, a novel message authentication scheme for multiple mobile devices in intelligent connected vehicles based on edge computing is proposed. The task of processing data in the vehicle is migrated to mobile devices, and tasks are executed utilizing the computing resources of multiple mobile devices in the edge computing model. The vehicle use certificate less ring signature technology to ensure the integrity of data processed by mobile devices. A security analyses show that our proposed schemes are secure in the random oracle model and can resist two types of adversaries under certificate less public key encryption. One type of adversary may be able to replace the mobile device's public key and the other type of adversary has access to the system master key.

Y. Wang et al., [3] Due to the broadcasting property of visible light communication (VLC) channels, VLC systems are under the threat of eavesdropping and malicious attack. In this study, the authors present an uncoordinated chaotic channel scrambling scheme to enhance the physical layer security for a multiple-input, multiple-output based VLC system. With the authors design, the legitimate receiver can self-descramble the data with the location information

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 2, February 2020

shared between the transceivers, and the eavesdroppers cannot retrieve the information without the secret key. The authors firstly embed the location information into the chaotic channel scrambling matrix, and then apply the non-negative orthogonal factorisation method to improve both the reliability and the security. Notably, with the aid of the shared location information, the received data can be self-descrambled and thus the uncoordinated channel scrambling could be realised. The theoretical security performances including the information leakage and the secrecy capacity are analysed and the simulation results demonstrate that the proposed scheme achieves higher security and more reliable performances compared with the counterpart schemes.

H. Taha et al.,[4] In wireless communication systems, the conventional secret key exchange is based on the public key cryptography, which requires complex computations to retain the secrecy level of these key bits. The proposed physical layer-based algorithms have shown promising performance to extract secret keys from the privately shared randomness relying on the reciprocal channel state between both communicated nodes. In this study, the authors propose a physical layer key exchange method which transmits the key bits by encoding them within some phase randomisation (PR) sequences that are privately indexed to a specific channel criterion. The PR sequences only randomise the data phases and thus no efficiency reduction will be incurred. In fact, by choosing a pool of randomisation sequences with certain statistical properties, they could also be used to condition the signal to meet physical layer transmission requirements such as bandwidth, envelope and so onThe results reveal that, relative to existing techniques, the proposed method offers superior key error rate performance at lower computational complexity with better secrecy level.

M. A. M. Abdullah, et al., [5] This work presents a novel security architecture for protecting the integrity of iris images and templates using watermarking and visual cryptography (VC). The proposed scheme offers a complete protection framework for the iris biometrics which consists of two stages: the first stage is for iris image protection, while the second is for the iris template. First, for protecting the iris image, a watermark text which carries personal information is embedded in the middle band frequency region of the iris image using a novel watermarking algorithm that randomly interchanges multiple middle band pairs of the discrete cosine transform. Second, for iris template protection, the binary iris template is divided into two shares using VC, where one share is stored in the database and the other is kept with the user on a smart card. In addition, the SHA-2 hash function is utilized to maintain the integrity of the stored iris template in both the database and smart card. The experimental and comparison results on the CASIA V4 and UBIRIS V1 iris databases demonstrate that the proposed framework preserves the privacy of the iris images and templates and retains robustness to malicious attacks.

M. Poolakkaparambil, et al., [6] This work presents a novel low-complexity cross parity code, with a wide range of multiple bit error correction capability at a lower overhead, for improving the reliability in circuits over GF(2 m). For an m input circuit, the proposed scheme can correct m $\leqslant$ D w $\leqslant$ 3 m/2 -1 multiple error combinations out of all the possible 2 m - 1 errors, which is superior to many existing approaches. From the mathematical and practical evaluations, the best case error correction is m/2 bit errors. Tests on 80-bit parallel and, for the first time, on 163-bit Federal Information Processing Standard/National Institute of Standards and Technology (FIPS/NIST) standard word-level Galois field (GF) multipliers, suggest that it requires only 106% and 170% area overheads, respectively, which is lower than the existing approaches, while error injection-based behavioral analysis demonstrates its wider error correction capability.

J. Xu, et al., [7] The original Number Theory Research Unit (NTRU) public key cryptosystem is vulnerable to multiple transmission attacks, and the designers of NTRU presented two countermeasures to prevent such attacks. In this study, the authors show that the first countermeasure is still not secure, the plaintext can be revealed by a linearisation attack technique. Moreover, they demonstrate that the first countermeasure is even not secure for broadcast attacks, a class of more general attacks than multiple transmission attacks. For the second countermeasure, they show that one special case of its padding function for the plaintext is also insecure and the original plaintext can be obtained by lattice methods.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 2, February 2020

S. N. Premnath et al.,[8] It is evaluate the effectiveness of secret key extraction, for private communication between two wireless devices, from the received signal strength (RSS) variations on the wireless channel between the two devices. it is use real world measurements of RSS in a variety of environments and settings. The results from our experiments with 802.11-based laptops show that in certain environments, due to lack of variations in the wireless channel, the extracted bits have very low entropy making these bits unsuitable for a secret key, an adversary can cause predictable key generation in these static environments, and in dynamic scenarios where the two devices are mobile, and/or where there is a significant movement in the environment, high entropy bits are obtained fairly quickly. Building on the strengths of existing secret key extraction approaches, it is develop an environment adaptive secret key generation scheme that uses an adaptive lossy quantizer in conjunction with Cascade-based information reconciliation and privacy amplification. Our measurements show that our scheme, in comparison to the existing ones that it is evaluate, performs the best in terms of generating high entropy bits at a high bit rate. The secret key bit streams generated by our scheme also pass the randomness tests of the NIST test suite that it is conduct.

Table 1: Summary of literature survey

Sr No.	Author Name & Year	Proposed Work	Outcome
1	Y. Yang, IEEE 2019	The period of the cascade connection is the period of the longest sequences it produces. An upper bound for the period of the cascade connection of a NFSR into a LFSR is established. In addition.	An n-stage NFSR is called an (n + n)-stage Grain-like NFSR, and two families of (n + n)stage Grain-like NFSRs such that the minimal period.
2	H. Zhong, IEEE 2019	A novel message authentication scheme for multiple mobile devices in intelligent connected vehicles based on edge computing.	High efficiency and applicability in practical intelligent connected vehicles system.
3	Y. Wang, IEEE 2018	An uncoordinated chaotic channel scrambling scheme to enhance the physical layer security for a multiple-input, multiple-output based VLC system.	The proposed scheme achieves higher security and more reliable performances compared with the counterpart schemes.
4	H. Taha, IEEE 2017	Physical layer- have extract secret keys from the privately shared randomness relying on the reciprocal channel state between both communicated nodes.	Method offers superior key error rate performance at lower computational complexity with better secrecy level.
5	M. A. M. Abdullah, IEEE 2016	A novel security architecture for protecting the integrity of iris images and templates using watermarking and VC.	The CASIA V4 and UBIRIS V1 iris databases demonstrate that the retains robustness to malicious attacks,
6	M. Poolakkaparambil, IEEE 2015	A novel low-complexity cross parity code, with a wide range of multiple bit error correction capability at a lower overhead, for improving the reliability in circuits over GF(2 m).	That it requires only 106% and 170% area overheads, respectively, which is lower than the existing approaches.
7	J. Xu, IEEE 2014	The designers of NTRU two countermeasures to prevent such attacks. In this study, the first countermeasure is still not secure,	One special case of its padding function for the plaintext is also insecure and the original plaintext can be obtained by lattice methods.
8	S. N. Premnath, IEEE 2013	The effectiveness of secret key extraction, for private communication between two wireless devices, from the RSS variations.	The secret key generation rate is increased when multiple sensors are involved in the key extraction process.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 2, February 2020

IV. CHALLENGES AND APPLICATIONS

A. Challenges

LTE communication takes place in an open access environment, which make VANETs more vulnerable to attacks that cause multiple threats to the security services. In particular, a Sybil attack is one of the most dangerous attacks in VANETs. This attack is the most influential attack that is addressed by the researchers. Maintaining the balance between privacy and non-repudiation is still required in order to detect Sybil attacks. In the past, many studies have been done on Sybil attacks. On the other hand, many other attacks such as jamming attacks and malware attacks in VANETs motivate further research. Many security challenges still exist, which need superior algorithms in order to solve these challenges. A robust authentication technique along with the message exchange approach is used to protect V2I and V2V communications from inside and outside attackers. The main problem occurs when the utilization of CA and TA and the schemes that rely on the private keys for V2X, i.e., V2V and V2I communications, can protect the vehicular network. However, it can increase the computational and transmission overheads and introduce the scalability challenges.

B. Applications

VANET applications can be divided into two major categories. Applications that increase vehicle safety on the roads are called safety applications. Applications that provide value-added services, for example, entertainment, are called user applications. In this article we concentrate only on applications with an important wireless networking component.

V. CONCLUSION

There is a great need for designing VANET algorithms in order to tackle all these challenges. Such algorithms can provide trustworthy communication on V2V and V2I, and also protect vehicle ID and location privacy. The future research directions for the VANET system should focus on security and privacy issues such as privacy preservation, trust management, location privacy, and so on. Such research directions require more time to study and conduct research in order to design and develop robust algorithms, which can tackle different kinds of security threats and challenges. In addition to these directions, the security systems must be enhanced by efficient authentication schemes for providing a secure communication. Additionally, an efficient intrusion detection system could be incorporated in vehicular networks to detect the malicious nodes and handle all types of security attacks.

REFERENCES

[1] Y. Yang, X. Zeng and Y. Xu, "Periods on the Cascade Connection of an LFSR and an NFSR," in Chinese Journal of Electronics, vol. 28, no. 2, pp. 301-308, 3 2019.

[2] H. Zhong, L. Pan, Q. Zhang and J. Cui, "A New Message Authentication Scheme for Multiple Devices in Intelligent Connected Vehicles Based on Edge Computing," in IEEE Access, vol. 7, pp. 108211-108222, 2019

[3] Y. Wang and L. Zhang, "Uncoordinated chaotic channel scrambling scheme for multiple-input, multiple-output-based VLC system," in IET Communications, vol. 12, no. 10, pp. 1245-1252, 26 6 2018.

[4] H. Taha and E. Alsusa, "Secret key establishment technique using channel state information driven phase randomisation in multiple-input multiple-output orthogonal frequency division multiplexing," in IET Information Security, vol. 11, no. 1, pp. 1-7, 1 2017.

[5] M. A. M. Abdullah, S. S. Dlay, W. L. Woo and J. A. Chambers, "A Framework for Iris Biometrics Protection: A Marriage Between Watermarking and Visual Cryptography," in IEEE Access, vol. 4, pp. 10180-10193, 2016.

[6] M. Poolakkaparambil, J. Mathew, A. M. Jabir and D. K. Pradhan, "A Low-Complexity Multiple Error Correcting Architecture Using Novel Cross Parity Codes Over GF(2^{m})," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 23, no. 8, pp. 1448-1458, Aug. 2015.

[7] J. Xu, L. Hu, S. Sun and Y. Xie, "Cryptanalysis of countermeasures against multiple transmission attacks on NTRU," in IET Communications, vol. 8, no. 12, pp. 2142-2146, 14 August 2014.

[8] S. N. Premnath et al., "Secret Key Extraction from Wireless Signal Strength in Real Environments," in IEEE Transactions on Mobile Computing, vol. 12, no. 5, pp. 917-930, May 2013.

[9] B. Fortescue and G. Gour, "Reducing the Quantum Communication Cost of Quantum Secret Sharing," in IEEE Transactions on Information Theory, vol. 58, no. 10, pp. 6659-6666, Oct. 2012.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 2, February 2020

[10] T. Liu and W. Tsai, "Quotation Authentication: A New Approach and Efficient Solutions by Cascaded Hashing Techniques," in IEEE Transactions on Information Forensics and Security, vol. 5, no. 4, pp. 945-954, Dec. 2010.

[11] J. H. Cheon, N. Jho, M. Kim and E. S. Yoo, "Skipping, Cascade, and Combined Chain Schemes for Broadcast Encryption," in IEEE Transactions on Information Theory, vol. 54, no. 11, pp. 5155-5171, Nov. 2008.

[12] A. Jabir, D. Pradhan, T. L. Rajaprabhu and A. K. Singh, "A Technique for Representing Multiple Output Binary Functions with Applications to Verification and Simulation," in IEEE Transactions on Computers, vol. 56, no. 8, pp. 1133-1145, Aug.2007,