A STUDY EVALUATING THE PERFORMANCE OF THE TPGF PROTOCOL AND ITS VARIANTS

Long Tran Huy*, Chinh Tran Thien* Hoai Trung Tran+
* Posts and Telecommunications Institute of Technology, Hanoi, Vietnam
+ University of Transport and Communications, Hanoi, VietNam

Abstract: In wireless multimedia sensor networks, the development of secure and energy-efficient routing protocols is of particular importance due to the sensitive nature of transmitted data and the resource limitations of sensor nodes. The Two Phase Geographic Forwarding Protocol (TPGF) [1] is a routing protocol based on geographic principles, aimed at improving multimedia data transmission. However, attacks on the protocol have also been identified, and its variants have been developed to address different security objectives. In this paper, we conduct an evaluation and simulation to highlight the trade-off performance metrics of routing protocols for application and deployment in specific scenarios**.**

Keywords: TPGF, CRC, Secu-TPGF, LS-TPGF, ECDSA-TPGF, MAC, Security, Routing, WMSN.

I. INTRODUCTION

Nowadays, the emergence of Wireless Sensor Network (WSN) is one of the dominant technology trends in the coming decades. Sensor technology combined with processing power and wireless communication will make WSN profitable to exploit in the future. WSN is considered one of the most important technologies of the 21st century. In the past decades, WSN has received great attention from academia and industry worldwide. WSN differs from conventional wireless networks in terms of a very large number of nodes, limited computing power, memory space, energy consumption, bandwidth, and communication capabilities. These unique characteristics make WSNs challenging when it comes to network security. In WSN, routing is the process of finding the best route to deliver data from the source node to the destination node, in which data traffic is routed from sensor nodes to the Sink node. These nodes are often limited in energy, storage, and computing resources, so they require efficient use. Therefore, there are many factors affecting the routing protocol such as node deployment, fault tolerance, scalability, data aggregation, loop routing, and energy constraints. Accordingly, secure routing needs to be considered an important factor in achieving secure routing in WSNs in general and multimedia wireless sensor networks (WMSNs) in particular. This requirement stems from the vulnerability of transmitted information and the inherent limitations of resources, especially the available energy and computing resources of sensor nodes. WMSNs are often deployed in contexts with strict requirements on reliability and security, including environmental monitoring, healthcare, military operations, and other important missions, where the transmitted data is not only meaningful but also requires accurate and secure transmission [2][3]. The constraints associated with WMSNs require that the selection and design of protocols prioritize two important factors: energy efficiency and data security [4]. At the same time, protecting message transmissions from threats such as spoofing, Sybil attacks, or wormhole attacks is necessary, because the data transmitted in WMSNs includes high-fidelity audio, images, and videos [5].

Recent advancements in the WMSN sector have yielded numerous secure routing protocols that offer optimized solutions addressing both security and energy consumption. Among these, adaptations of TPGF have garnered significant attention due to their capability to effectively route based on geographic positioning, integrated with robust security frameworks such as identity-based non-interactive key distribution system (ID-NIKDS) and message authentication code (MAC) [6]. Protocols like Secured Two Phase Geographic Forwarding Protocol (SecuTPGF) [6], Lightweight secure routing based on the TPGF (LS-TPGF) [7] and Elliptic Curve Digital Signature Algorithm base the TPGF (ECDSA-TPGF) [8], exemplify the equilibrium between robust security measures and energy efficiency. These protocols not only resolve critical security challenges but are also engineered to reduce latency and energy usage, thereby ensuring their practical application in contemporary wireless sensor networks [9].

In light of the escalating utilization of varied applications within WMSNs, routing protocols that are both secure and efficient and capable of fulfilling the performance demands of these applications are necessary. The assessment and comparison of routing protocols' performance is imperative for their effective implementation. To our knowledge, no comprehensive research has been conducted that rigorously evaluates the performance of the three protocols—SecuTPGF, LS-TPGF, and ECDSA-TPGF. Consequently, this investigation seeks to bridge this research void by analyzing the appropriateness of these routing protocols with regard to security, latency mitigation, and energy efficiency across a variety of application contexts.

Contact author: Long Tran Huy
Email: longth@ptit.edu.vn

Manuscript received: 10/2024, revised: 11/2024, accepted: 11/2024.

II. RELATED WORK

When researching and building routing protocols for WMSNs, these protocols often consider the balance between security and energy. Depending on the specific application, these protocols will be designed to ensure security but also ensure that the network lifetime is optimal. These networks are often deployed in important applications that require high security levels such as healthcare and military operations. The transmitted data can be affected by various threats, including spoofing and Sybil attacks. Therefore, a secure and efficient routing protocol needs to be designed to prolong the network lifetime while preventing as many attacks as possible [8], [10]. There have been many studies on building routing security mechanisms for WMSNs. Notably, variations of the TPGF protocol are becoming more and more prominent. TPGF uses location to improve routing efficiency, making it particularly suitable for resource-constrained environments [11]. Protocols such as SecuTPGF, LS-TPGF, and ECDSA-TPGF are good examples of this tradeoff, combining strong security mechanisms while ensuring optimized energy consumption. For example, SecuTPGF has been carefully designed to address critical security issues in WMSNs by adopting a lightweight cryptographic approach that enhances both security and energy efficiency [2]. The LS-TPGF protocol further improves routing security by demonstrating resilience against malicious nodes that can engage in selective packet dropping, thereby ensuring reliable data delivery [3]. Similarly, ECDSA-TPGF uses the Elliptic Curve Digital Signature Algorithm to enhance security without compromising energy efficiency, which is crucial for the robustness of sensor networks [4].

Furthermore, integrating frameworks such as Identity-based Non-Interactive Key Distribution System (ID-NIKDS) enhances data security by enabling secure key distribution, which is crucial in protecting communication channels in WMSNs [12]. Secure and efficient routing protocols remain a key challenge as the Internet of Things (IoT) and WSNs continue to evolve. One such example is a secure and energy-efficient routing protocol based on micro-segmentation and batch authentication that uses the Supremum Distance K-Prototype (SD-KP) algorithm and Elliptic Curve Cryptography (ECC) for secure data transmission and optimizes routing with the LGWI-GEAR algorithm [13]. Genetic algorithm-based secure routing protocols optimize route selection by balancing security and energy efficiency, demonstrating resilience to attacks, and improving network performance metrics such as packet delivery ratio [14]. These protocols represent a significant advance in securing wireless multimedia sensor networks while maintaining energy efficiency, which is critical for deployment in resource-constrained and sensitive environments.

III. THE FUNDAMENTAL OPERATIONS OF TPGF AND ITS VARIANT PROTOCOLS

A. *The TPGF protocol [1]*

The TPGF protocol constitutes a framework for routing that is oriented toward geographic principles, with the objective of improving the transmission of multimedia data within WMSNs. TPGF functions through two principal phases.

- Geographic Greedy Forwarding: TPGF adopts a greedy forwarding strategy, wherein each forwarding node identifies the neighboring node that is nearest to the sink, thereby circumventing intricate planar geometric regulations. This methodology alleviates the "Local Minimum" issue and incorporates two fundamental techniques:

+ Greedy Forwarding: The forwarding node consistently opts for the next hop that is closest to the sink.

+ Step Back and Mark technique is activated when greedy forwarding fails to identify an appropriate next hop.

- Path Optimization of this phase is to minimize the presence of superfluous nodes along the routing path to decrease end-to-end latency. Only those nodes with the most significant path and hop counts are preserved for data transmission, thereby facilitating effective communication.

TPGF possesses the capability to manage dynamic holes that emerge when specific sensor nodes are burdened due to multimedia data transmission. Accommodates multiple non-interfering pathways to improve transmission efficacy and mitigate congestion, which is particularly critical for extensive multimedia data. Guarantees the employment of the most direct routes, thus reducing end-to-end delay for real-time multimedia applications.

The TPGF protocol consists of two distinct phases: geographic forwarding and path optimization. The source node seeks out the nearest available neighbor toward the sink and persists in forwarding until it encounters an obstruction, at which point it activates the "step back & mark" strategy. Upon establishing the routing path, nodes along this route dispatch confirmation messages, retaining solely the optimal nodes for data forwarding, thereby eliminating extraneous loops.

B. *The secuTPGF protocol [7]*

SecuTPGF protocol is an advancement of the original TPGF protocol, integrating identity-based security mechanisms to bolster neighbor discovery and routing security within WMSNs. SecuTPGF employs the Identity-Based, Non-Interactive Key Distribution Scheme, which enables nodes to generate symmetric keys securely with minimal information exchange. This protocol safeguards nodes against external threats and mitigates the effects of insider attacks by merging identity authentication with symmetric key establishment to facilitate secure communication. Otherwise, a message authentication code (MAC) is utilized in SecuTPGF to ensure both message integrity and authenticity. MACs are produced using a shared secret key among nodes, and intermediary nodes recalculate the MAC during message forwarding to maintain the continuous integrity of the messages.

SecuTPGF employs comprehensive defense mechanisms to protect networks from diverse security threats by ensuring that only authorized nodes with unique secret keys can access the network, thereby fostering node authenticity. Furthermore, it implements stringent measures against impersonation, Sybil, wormhole, and selective forwarding attacks, ultimately enhancing the network's overall resilience through improved authentication and secure data transmission.

C. The LS-TPGF protocol [8]

LS-TPGF constitutes a security-centric routing protocol specifically designed for WMSNs, employing lightweight cryptographic methodologies such as Cyclic Redundancy Check (CRC) and Elliptic Curve Cryptography (ECC) to facilitate effective node authentication while ensuring the integrity of messages with minimal computational demands.

The protocol effectively addresses wormhole attacks through latency assessments and distance validation, mitigates Sybil attacks by enforcing exclusive I.D.s and rigorous authentication, and safeguards against selective forwarding attacks by persistently monitoring the forwarding conduct of neighboring nodes and isolating non-compliant entities. By employing lightweight cryptographic techniques that are appropriate for resource-constrained devices, LS-TPGF enhances the dependability and security of WMSNs, effectively tackling both operational limitations and the rigorous security requisites of contemporary wireless sensor networks in multimedia contexts.

D. The ECDSA-TPGF protocol [9]

ECDSA-TPGF is an enhanced version of the TPGF protocol, meticulously designed to secure routing in Wireless Multimedia Sensor Networks (WMSNs). This protocol synergistically combines elliptic curve-based digital signatures (ECC) and cyclic redundancy check (CRC) mechanisms to authenticate nodes and messages within the network.

To prevent attacks, ECDSA-TPGF employs robust mechanisms: it mitigates spoofing attacks by ensuring only nodes with valid public keys and digital signatures can participate in the network; it prevents Sybil attacks by enforcing unique IDs and authentication for each node; and it safeguards against wormhole and selective forwarding attacks by using digital signatures and CRC codes to ensure message integrity and authenticity, thereby preventing message tampering or blocking. Through these integrated security measures, ECDSA-TPGF significantly enhances the resilience and reliability of WMSNs against common network threats.

E. Evaluate

From the research results of the authors [1], [2], [3], [4], it is possible to compare the routing protocols TPGF, SecuTPGF, LS-TPGF and ECDSA-TPGF, based on the attacks and design parameters as shown in Table I and Table II below:

Table I. Comparison based on design parameters

Parameter	TPGF	SecuTPGF	LS-TPGF	ECDSA-TPGF
Network type	WMSN	WMSN	WMSN	WMSN
Overhead (computation Cost)	Low	High	Lower than Secu-TPGF	Lower than Secu-TPGF
Security	Low	High	High	High
Scalability	Good	Good	Good	Good
End-to-end delay	Low	High	Lower than Secu-TPGF	Lower than Secu-TPGF

Table II. Comparison based on attacks

Parameter	TPGF	SecuTPGF	LS-TPGF	ECDSA-TPGF
Spoofing	No	Yes	Yes	Yes
Sybil Attack	No	Yes	Yes	Yes
Wormhole Attack	No	Yes	Yes	Yes
Flooding	No	Yes	Yes	Yes

By comparing both cases in terms of design and security parameters, it can be seen that LS-TPGF and ECDSA-TPGF are more efficient than Secu-TPGF and TPGF. The two protocols LS-TPGF and ECDSA-TPGF were developed mainly to save energy and ensure security when routing attacks occur. Meanwhile, TPGF does not apply any security mechanism, so if no attack occurs, it is much more efficient than the remaining protocols. However, when some nodes in the network are attacked and become malicious nodes, they can increase the end-to-end delay of the message by randomly forwarding the request message and avoiding path optimization in the confirmation message. This makes TPGF no longer secure and more efficient than other protocols.

IV. EXPERIMENTAL EVALUATIONS

With the aim of evaluating the performance of the protocols, we opted for the MATLAB simulator due to its extensive application in simulating and processing data, particularly in wireless sensor networks [15]. We employ discrete numerical simulations within a network scenario measuring 640x400 m, utilizing the simulation parameters delineated in Table III below. We will sequentially examine the delay and energy consumption metrics associated with the routing protocols.

Table III. Simulation parameters [2]

Parameter	Value
Network size	640 x 400 m
Number of sensor nodes	100 - 1000
Number of base station	1
Number of source nodes	1
Initial Energy of sensor nodes	10 J
Transmission radius	60 - 120 m
Expected lifetime	1 - 14 h

A. Delay evaluations

Table IV shows the simulation results comparing the average delay of SecuTPGF, LS-TPGF, ECDSA-TPGF, and TPGF protocols when the number of nodes of these protocols changes.

Table IV. Average latency

Num Nodes	Secu-TPGF	LS-TPGF	ECDSA-TPGF	TPGF
0	0	0	0	0
100	0.04896	0.03264	0.03264	0.0272
200	0.06273	0.04182	0.04182	0.03485
300	0.03138	0.02092	0.02092	0.017433333
400	0.0352575	0.023505	0.023505	0.0195875
500	0.034992	0.023328	0.023328	0.01944
600	0.032085	0.02139	0.02139	0.017825
700	0.026742857	0.0178286	0.017828571	0.0148571
800	0.0297225	0.019815	0.019815	0.0165125
900	0.02778	0.01852	0.01852	0.0154333
1000	0.028773	0.019182	0.019182	0.015985

Figure 1 presents the obtained delay for SecuTPGF, LS-TPGF, ECDSA-TPGF, and TPGF protocols.

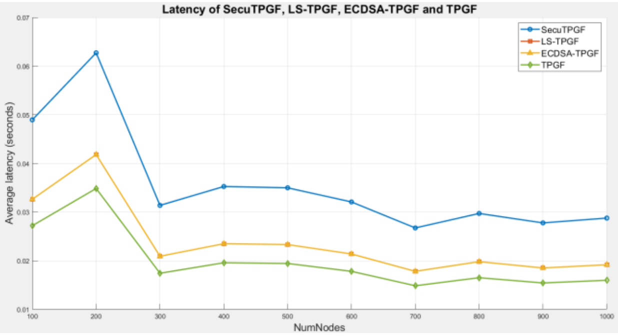

Figure 1. Latency of SecuTPGF, LS-TPGF, ECDSA-TPGF and TPGF protocols

Simulation results indicate that the introduction of security mechanisms into the TPGF protocol leads to an increase in average delay for all secure protocols. LS-TPGF and ECDSA-TPGF exhibit similar average delays and outperform SecuTPGF in terms of latency. As the number of nodes increases, the source nodes will be able to select more optimal routes. Accordingly, the delay will tend to decrease and stabilize as the number of nodes increases.

B. Energy evaluations

Table V and Figure 2 present the simulation results for the average energy consumption of SecuTPGF, LS-TPGF, ECDSA-TPGF, and TPGF protocols.

Table V. Average energy consumption of SecuTPGF, LS-TPGF, ECDSA-TPGF and TPGF protocols

Num Nodes	Secu-TPGF	LS-TPGF	ECDSA-TPGF	TPGF
0	0	0	0	0
100	0.5984	0.4352	0.4896	0.1632
200	0.7667	0.5576	0.6273	0.2091
300	0.38353333	0.2789333	0.3138	0.1046
400	0.430925	0.3134	0.352575	0.117525
500	0.42768	0.31104	0.34992	0.11664
600	0.39215	0.2852	0.32085	0.10695
700	0.32685714	0.2377143	0.267428571	0.0891428
800	0.363275	0.2642	0.297225	0.099075
900	0.33953333	0.2469333	0.2778	0.0926
1000	0.35167	0.25576	0.28773	0.09591

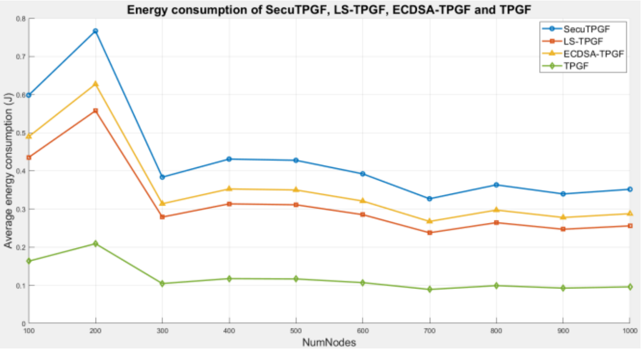

Figure 2. Energy consumption of SecuTPGF, LS-TPGF, ECDSA-TPGF and TPGF protocols

Simulation results indicate that the secure protocols (SecuTPGF, LS-TPGF, and ECDSA-TPGF) consume more average energy compared to the original TPGF protocol. LS-TPGF and ECDSA-TPGF exhibit similar energy consumption levels, outperforming SecuTPGF in terms of energy efficiency. The simulation results also show that as the number of nodes increases, the ability to select more routes leads to a reduction in the overall energy consumption of the network.

C. Discussions

Attack preventions: The SecuTPGF protocol utilizes MAC for the authentication of routing packets, thereby safeguarding their integrity and mitigating risks associated with spoofing, modification, Sybil, wormhole, and information spoofing attacks through the verification of both node identities and packets. Nevertheless, the employment of MAC entails more intricate computations and higher resource utilization, which escalates computational expenses and energy consumption. Conversely, LS-TPGF integrates Cyclic Redundancy Check (CRC) and Elliptic Curve Cryptography (ECC) to uphold information integrity and security. CRC expedites error detection, whereas ECC offers enhanced security with reduced key sizes, assisting in the defense against data spoofing and modification attacks while optimizing energy usage. ECDSA-TPGF leverages elliptic curve-based digital signatures for the authentication of nodes and routing messages, providing superior security and resource efficiency in comparison to SecuTPGF.

Performance aspect: SecuTPGF delivers formidable security but necessitates substantial computational resources, resulting in increased latency and diminished overall performance. LS-TPGF emphasizes more efficient techniques such as CRC to enhance performance and conserve Energy, consequently prolonging the operational lifespan of sensor nodes. ECDSA-TPGF exhibits enhanced efficiency in authentication due to the utilization of shorter elliptic keys, though it may incur marginally higher latency than LS-TPGF. Resource and Energy Efficiency SecuTPGF imposes significant demands on computational resources and has elevated energy consumption, rendering it less suitable for applications that necessitate prolonged sensor node lifespans. Both LS-TPGF and ECDSA-TPGF incorporate ECC and CRC, which contribute to energy savings and an extended lifespan for sensor nodes, with ECDSA-TPGF demonstrating comparable or superior resource efficiency relative to LS-TPGF.

Complexity: SecuTPGF is characterized by a computational complexity of $O(k^3+n)$ owing to the implementation of pairing on elliptic curves and MAC. In contrast, LS-TPGF and ECDSA-TPGF exhibit a complexity of $O(k^2+n)$, with LS-TPGF employing less intensive computations and ECDSA-TPGF offering enhanced security through digital signatures. While ECDSA-TPGF presents greater complexity than LS-TPGF, it is still less demanding than SecuTPGF due to the shorter key sizes associated with ECC.

V. CONCLUSION

In summary, this paper has conducted a comprehensive evaluation and simulation analysis to compare the performance of variants of the original TPGF routing protocol including SecuTPGF, LS-TPGF, and ECDSA-TPGF. The evaluation results show that SecuTPGF ensures the highest level of security, but consumes more energy than the remaining protocols. In contrast, LS-TPGF and ECDSA-TPGF provide a reasonable balance between security and performance, especially suitable for WSNs with limited resources. The results of the paper also provide a basis for choosing a secure protocol to deploy for WMSNs in practice. In the future, the authors will continue to research lightweight cryptographic solutions towards creating very lightweight installation solutions, but without sacrificing too much security to keep up with and match the rapid development needs of WSNs.

REFERENCES

[1] Lei Shu, Yan Zhang, Laurence T. Yang, YuWang, Manfred Hauswirth, Naixue Xiong, *TPGF: geographic routing in wireless multimedia sensor networks*, Telecommun Syst (2010) 44: 79–95.

[2] Ahmed HA, Al-Asadi HA, *An Overview of Routing Protocols Performance in Wireless Multimedia Sensor Networks*, 3rd Information Technology To Enhance e-learning and Other Application (IT-ELA). 2022 Dec 27:133-9.

[3] Nur FN, Moon NN, Chakraborty NR, *A survey on routing protocols in wireless multimedia sensor networks*, International Journal of Computer Applications. 2013 Jan 1;73(11).

[4] Ilyas M, Ullah Z, Khan FA, Chaudary MH, Malik MS, Zaheer Z, Durrani HU, *Trust-based energy-efficient routing protocol for Internet of things–based sensor networks*, International Journal of Distributed Sensor Networks. 2020 Oct;16(10):1550147720964358.

[5] Chiwariro R, N T, *Quality of service aware routing protocols in wireless multimedia sensor networks: survey*, International Journal of Information Technology. 2022 Mar;14(2):789-800.

[6] Taye Mulugeta1, Lei Shu, Manfred Hauswirth, Min Chen, Takahiro Hara, Shojiro Nishio, *Secured Two Phase Geographic Forwarding Protocol in Wireless Multimedia Sensor Networks, 2010 IEEE Global Telecommunications Conference GLOBECOM 2010.*

[7] Long Tran Huy, Chinh Tran Thien, Hoai Trung Tran, *A novel lightweight secure routing based on the TPGF for WMSNs*, Journal of Science and Technology on Information and Communications, No.03 (CS.01) 2023.

[8] Long Tran Huy, Chinh Tran Thien, Hoai Trung Tran, Vinh Pham Van, *A novel security routing using identity-based lightweight digital signature in WMSNs*, Journal of Science and Technology, Hanoi University of Industry, volume 59, number 6A (2023).

[9] Kumar A, Zhao M, Wong KJ, Guan YL, Chong PH, *A comprehensive study of IoT and WSN MAC protocols: Research issues*, challenges and opportunities, IEEE Access. 2018 Nov 25;6:76228-62.

[10] Jaydip, Sen., Arijit, Ukil, *A secure routing protocol for wireless sensor networks*, (2010).277-290. doi: 10.1007/978-3-642-12179-1_25.

[11] Ashish, Bagwari., Menka, Goswami., Anil, Kumar, *Anlytical study based on issues of Routing & Security in Wireless sensor networks*, Network and Complex Systems, (2014).;4(4):30-35.

[12] Steinwandt R, Suárez Corona A, *Identity-based non-interactive key distribution with forward security*, Designs, Codes and Cryptography. 2012 Jul; 64:195-208.

[13] Khaleel-Ur-Rahman, Khan., M.A., Azeem, *An optimized crypto-based routing protocol for secure routing in wireless sensor networks*, Concurrency and Computation: Practice and Experience, (2024). doi: 10.1002/cpe.8067

[14] Amit, Singh., Dr., Devendra, Singh, *Genetic Algorithm-Based Secure Routing Protocol for Wireless Sensor Networks*. (2023). doi: 10.47392/irjaeh.2023.007.

[15] Q. Ali, Akram Abdulmaowjod, H. Mohammed, Simulation & performance study of wireless sensor *network (WSN) using MATLAB*, 1st International Conference on Energy, Power and Control (EPC-IQ) 2010.

NGHIÊN CỨU ĐÁNH GIÁ HIỆU SUẤT CỦA GIAO THỨC TPGF VÀ CÁC BIẾN THỂ CỦA NÓ

Tóm tắt: Trong mạng cảm biến đa phương tiện không dây, việc xây dựng các giao thức định tuyến bảo mật và tiết kiệm năng lượng có tầm quan trọng đặc biệt do tính chất nhạy cảm của dữ liệu được truyền tải và các giới hạn tài nguyên của các nút cảm biến. Giao thức chuyển tiếp địa lý hai pha (TPGF) [1] là một giao thức định tuyến dựa trên các nguyên tắc địa lý, với mục tiêu cải thiện việc truyền dữ liệu đa phương tiện. Tuy nhiên, các vấn đề tấn công vào giao thức cũng đã được chỉ ra và các biến thể của nó đã được phát triển cho các mục tiêu bảo mật khác nhau. Trong bài báo này, chúng tôi thực hiện đánh giá và mô phỏng để chỉ ra các chỉ số đánh đổi về hiệu năng của các giao thức định tuyến nhằm ứng dụng và triển khai trong các kịch bản cụ thể.

Từ khóa: TPGF, CRC, Secu-TPGF, LS-TPGF, ECDSA-TPGF, MAC, Security, Routing, WMSN.

Long Tran Huy received an electronics and telecommunications engineer from Electric Power University, in 2013 and a Master's degree from Posts and Telecommunications Institute of Technology in 2015. Currently, he is a postgraduate of the University of Communications and Transport, Hanoi. He is a lecturer at the Faculty of Telecommunications 1 - Institute of Post and Telecommunications Technology. His current research interest is information security, Routing security, wireless communications, WSN, UAV, and IoT.

Email: longth@ptit.edu.vn

Chinh Tran Thien was born in 1967. He got a Bachelor's degree from the University of Transport and Communications (UTC) in 1991 and hold visiting lecturers at the University. He then got a Ph.D. specialist in "Networks and Communications" from the Posts and Telecommunications Institute of Technology in 2005. Currently, he is deputy director of the Research Institute of Posts and Telecommunications. Main research directions: Research and development of Internet of Things (IoT) applications in the fields of telecommunications, smart transportation, smart agriculture, intelligent environment management, smart health, etc. Research and development of security and security applications in information communication technology (ICT), which focus on wireless sensor networks (WSN). Research and develop processing, control, and automation systems. Which focus on smart city, smart transportation.

Email: trthchinh@gmail.com

Hoai Trung Tran was born in 1976. He is the Deputy Head of the Department of Telecommunications Engineering, Faculty of Electrical - Electronic Engineering - University of Transport and Communications. His research directions are advanced wireless communication: cooperative and cognitive communication, mm-wave communication; digital signal processing, design, and production of wireless transceivers: beamforming, multiantenna, hybrid precoder, space-time coding, and spatial filter, massive MIMO, F- OFDM, FPGA, etc.; application of new technologies integrated by information, communication, and electronics such as WSN; telecommunication using artificial intelligence and deep learning.

Email: trungth@utc.edu.vn.