ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2023.0432

A NOVEL EFFICIENT SECURITY VERIFICATION TECHNIQUE BASED ON SERVICE PACKAGE IDENTIFIER IN WIRELESS MOBILE AD-HOC NETWORKS

H.C. Kantharaju[1], V.V. Apurva[2], B. Gopinathan[3] and A. Nallathambi[4]
[1]*Department of Artificial Intelligence and Machine Learning, Vemana Institute of Technology, India*
[2]*Department of Computer Science, Acharya Bangalore B School, India*
[3]*Department of Computer Science and Engineering, Adhiyamaan College of Engineering, India*
[4]*Department of Electronics and Communication Engineering, Roever Engineering College, India*

Abstract

This paper presents a novel and efficient security verification technique for Wireless Mobile Ad-Hoc Networks (MANETs) using The Service Package Identifier (SPI). The dynamic and self-organizing nature of MANETs makes them susceptible to a variety of security threats. Using the SPI, the proposed technique authenticates and verifies the integrity of service bundles exchanged between network nodes. By employing the SPI as a unique identifier for each service packet, the technique protects against unauthorized access and data tampering and ensures secure communication. The experimental results demonstrate the efficacy and efficiency of the proposed technique, which offers improved MANET security and resiliency.

Keywords:

Security Verification, Service Package Identifier, Authentication, Integrity, Secure Communication, Unauthorized Access, Data Tampering, Resilience

1. INTRODUCTION

Wireless Mobile Ad-Hoc Networks (MANETs) have attracted considerable interest in recent years due to their ability to provide flexible and decentralized communication without requiring infrastructure. MANETs consist of a collection of mobile nodes that form a network dynamically, allowing for communication in situations where a fixed infrastructure is unavailable or impractical. However, the characteristics inherent to MANETs, such as their dynamic topology, limited resources, and lack of centralized control, pose significant security challenges [1]-[3].

MANETs are susceptible to a variety of security hazards, including eavesdropping, unauthorized access, data tampering, and network disruption, making security a top priority. Traditional security mechanisms designed for wired or infrastructure-based wireless networks may not be viable for MANETs due to their unique characteristics [4]. Consequently, there is a need for innovative and effective security techniques that are specifically tailored to address the challenges of MANETs [5].

The purpose of this study is to propose a Service Package Identifier (SPI)-based technique for efficient security verification in MANETs. The SPI is a unique identifier for service bundles that are exchanged between network nodes. The proposed technique aims to provide authentication and integrity verification to assure secure communication in MANETs by leveraging the SPI.

This research concentrates on the development of an SPI-based security verification technique for MANETs. The method seeks to increase the security and resilience of MANETs by addressing the challenges of authentication, integrity, and secure communication. Simulations will be used to assess the efficacy and efficiency of the proposed technique in comparison to existing approaches.

This novel technique has the potential to provide a robust and reliable security solution for a variety of applications, including military operations, disaster response, and emergency communication systems, by addressing the security concerns unique to MANETs. The following sections of this paper will provide an exhaustive review of existing techniques, a detailed description of the proposed security verification technique, experimental results, and a discussion of the implications and future directions of the research.

2. BACKGROUND

MANETs are a promising communication paradigm that enables mobile devices to establish a network infrastructure without relying on a centralized infrastructure. Each node in a MANET functions as both a host and a router, enabling direct data transmission between nodes. This decentralized character makes MANETs appropriate for situations where traditional wired networks or infrastructure-based wireless networks are impractical or unavailable, such as disaster-stricken areas, military operations, and sensor networks [6]-[8].

MANETs provide numerous benefits, including increased adaptability, scalability, and deployment speed. Nevertheless, due to their dynamic topology, limited resources, lack of centralized control, and susceptibility to a variety of malevolent attacks, these networks present unique security challenges [9]. MANETs are susceptible to threats including surveillance, spoofing, data tampering, and denial-of-service attacks due to the lack of a fixed infrastructure and the open nature of communication.

Traditional security mechanisms designed for tethered or infrastructure-based wireless networks do not apply directly to MANETs. The self-organizing and dynamic nature of MANETs necessitates the use of novel security techniques that can adapt to changing network conditions and effectively defend against a variety of attacks [10]. To ensure secure and dependable communication, there is a need for efficient security verification techniques that are specifically tailored for MANETs.

Diverse strategies, including encryption algorithms, routing protocols, and intrusion detection systems, have been employed to address the security challenges posed by MANETs [11]. Nevertheless, these approaches frequently introduce additional overhead, consume network resources, and may not completely mitigate the security hazards in MANETs. To protect the integrity and confidentiality of data in MANETs, it is necessary to develop

novel techniques that establish a balance between security, efficiency, and resource utilization [12].

This research intends to propose a novel security verification technique based on the Service Package Identifier (SPI) to resolve the unique security concerns in MANETs. By leveraging the SPI unique identifier, the proposed technique aims to provide efficient authentication and integrity verification to assure secure communication between nodes. In the subsequent sections of this paper, a thorough description of the proposed technique, its implementation, evaluation, and potential implications for enhancing the security of MANETs will be provided.

3. PROPOSED SECURITY VERIFICATION TECHNIQUE

The proposed security verification method employs the Service Package Identifier (SPI) as a unique identifier for service packages exchanged between MANET nodes. The SPI is essential for authenticating and confirming the integrity of service bundles, ensuring secure communication and protecting against unauthorized access and data tampering. A number of components constitute the technique, including SPI generation, authentication mechanism, integrity verification, and secure communication.

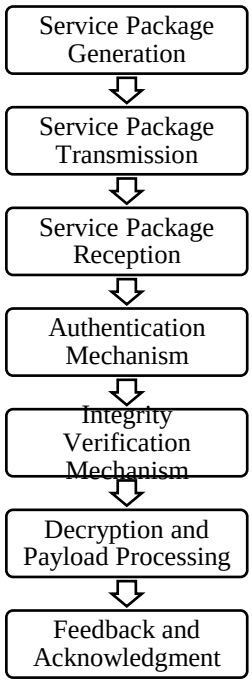

Fig.1. Security Verification

3.1 SERVICE PACKAGE IDENTIFIER (SPI)

The SPI is a unique identifier that is assigned to each service bundle in the MANET. It is generated by combining various packet attributes, such as the source node ID, the destination node ID, a timestamp, and a shared secret key between communicating nodes. The SPI is calculated using a hash function, ensuring the identifier uniqueness and integrity.

The SPI generation equation can be represented as follows:

$$SPI = Hash(source\_node\_ID + destination\_node\_ID + timestamp + secret\_key)$$

where:

Hash(): Represents a hash function that takes the concatenated attributes as input and produces a fixed-size hash value.

source_node_ID: Identifier of the source node.

destination_node_ID: Identifier of the destination node.

timestamp: Timestamp indicating the time of package generation.

secret_key: A shared secret key between the communicating nodes.

3.2 AUTHENTICATION MECHANISM

Using the SPI, the authentication mechanism verifies the authenticity of received service packages. The receiving node recalculates the SPI using the received attributes and the shared secret key with the source node after receiving a service package. The recalculated SPI is then compared to the SPI received in the container. If the two SPIs match, the delivery is deemed authentic, and communication is allowed to continue. Otherwise, the package is considered potentially malevolent and discarded.

The authentication equation can be expressed as follows:

$$Recalculated\_SPI = Hash(received\_source\_node\_ID + received\_destination\_node\_ID + received\_timestamp + secret\_key)$$

3.3 INTEGRITY VERIFICATION

Integrity verification ensures that the received service bundle was not altered during transmission. In addition to the authentication mechanism, a checksum or cryptographic hash function may be used to validate the package integrity. The checksum or hash value is computed on the entire packet, which includes the payload, header, and SPI. The receiving node compares the calculated checksum or hash value to the one contained within the packet. If they match, the package is deemed intact; otherwise, data tampering is possible.

The integrity verification equation can be represented as follows:

$$Checksum/Hash\_value = Calculate(package\_payload + package\_header + SPI)$$

3.4 SECURE COMMUNICATION

Once the authentication and integrity checks have been successfully conducted, the receiving node can trust the service package authenticity and integrity. Without worrying about unauthorized access, eavesdropping, or data manipulation, the secure communication between the nodes can proceed. The proposed method provides a robust and efficient method for establishing secure communication channels within the MANET, thereby augmenting the network overall security and resilience.

By incorporating SPI-based authentication and integrity verification mechanisms, the proposed technique offers MANETs an efficient and reliable security verification method. It mitigates the risks associated with unauthorized access, data manipulation, and other security threats in environments that are dynamic and resource-constrained. Through simulations and comparative studies, the subsequent sections of this paper will evaluate and

analyze the performance of the proposed technique in greater depth.

3.5 SECURE COMMUNICATION

The proposed security verification technique achieves secure communication by incorporating cryptographic algorithms and secure protocols. The architecture for secure communication includes encryption and decryption processes, as well as mechanisms for key exchange to establish secure channels between nodes.

3.5.1 Encryption and Decryption:

Before transmission, encryption is applied to the data payload of the service bundles to ensure confidentiality and prevent eavesdropping. Using a symmetric encryption algorithm, such as Advanced Encryption Standard (AES) or Data Encryption Standard (DES), the source node encrypts the payload. The encryption procedure utilizes a shared secret key that is only known to the sender and intended recipient.

The encryption equation can be represented as follows:

$$Encrypted\_Payload = Encrypt(Payload, Secret\_Key)$$

where, Encrypt() represents the encryption function that encrypts the payload using the secret key.

Upon receiving the encrypted payload, the recipient node applies the corresponding decryption process to retrieve the original data.

The decryption equation can be represented as follows:

$$Decrypted\_Payload = Decrypt(Encrypted\_Payload, Secret\_Key)$$

where, Decrypt() represents the decryption function that decrypts the encrypted payload using the secret key.

By encrypting and decrypting the payload, communication between nodes is secured and unauthorized access is prevented.

3.5.2 Key Exchange:

The establishment of secure channels and the exchange of cryptographic keys between communicating nodes are also required for secure communication. Protocols for key exchange, such as Diffie-Hellman or RSA, are frequently employed for this purpose.

Sender and recipient nodes generate their own public-private key pairs during the Diffie-Hellman key exchange. They exchange their public keys and use their private keys in conjunction with the received public key to generate a shared secret key. This shared secret key is subsequently employed for succeeding encryption and decryption operations.

The Diffie-Hellman equations for exchanging keys can be summed up as follows:

Algorithm 1: Sender/Receiver Node

```
#sender node
function sendPackage(destination_node_ID, payload):
    timestamp = getCurrentTimestamp()
    SPI = generateSPI(source_node_ID, destination_node_ID, timestamp, secret_key)
    encrypted_payload = encrypt(payload, secret_key)
    package = createPackage(source_node_ID, destination_node_ID, timestamp, SPI, encrypted_payload)
    send(package)
function generateSPI(source_node_ID, destination_node_ID, timestamp, secret_key):
    concatenated_attributes = concatenate(source_node_ID, destination_node_ID, timestamp)
    SPI = hash(concatenated_attributes + secret_key)
    return SPI
// Receiver Node
function receivePackage(package):
    received_source_node_ID = getPackageSourceNodeID(package)
    received_destination_node_ID = getPackageDestinationNodeID(package)
    received_timestamp = getPackageTimestamp(package)
    received_SPI = getPackageSPI(package)
    received_encrypted_payload = getPackageEncryptedPayload(package)
    recalculated_SPI = generateSPI(received_source_node_ID, received_destination_node_ID, received_timestamp, secret_key)
    if recalculated_SPI == received_SPI:
        decrypted_payload = decrypt(received_encrypted_payload, secret_key)
        processPayload(decrypted_payload)
    else:
        discardPackage()
function generateSPI(source_node_ID, destination_node_ID, timestamp, secret_key):
    concatenated_attributes = concatenate(source_node_ID, destination_node_ID, timestamp)
    SPI = hash(concatenated_attributes + secret_key)
    return SPI
```

Once the shared secret key has been derived via the key exchange procedure, it can be used for encryption and decryption as previously described.

By incorporating encryption, decryption, and key exchange mechanisms, the proposed method ensures the security of MANET communication channels. This architecture protects against unauthorized access, surveillance, and data tampering by providing confidentiality, authentication, and integrity for the exchanged data.

The encryption, hash calculation, timestamp retrieval and package creation functions exist. In addition, it assumes the availability of functions to extract attributes from the received package as well as functions to handle the processing of the payload and the discarding of packages.

The algorithm depicts the fundamental flow of the proposed technique, in which the sender node generates the SPI based on the package attributes and the secret key, encrypts the payload, and creates the package for transmission. The receiver node receives the package, recalculates the SPI with the received attributes and the shared secret key, verifies the integrity of the SPI, decrypts the payload if the SPI is valid, and then processes the payload.

The SPI is generated by the sender node and verified by the receiver node as part of the authentication mechanism in the pseudocode.

3.5.3 Sender Node:

- The sender node generates the SPI using the **generateSPI()** function.
- The SPI is calculated by concatenating the source node ID, destination node ID, timestamp, and secret key, and then applying a hash function (**hash()**).
- The generated SPI is included in the package along with the other attributes.

3.5.4 Receiver Node:

- The receiver node receives the package and extracts the received SPI, source node ID, destination node ID, timestamp, and encrypted payload.
- The receiver node recalculates the SPI using the same **generateSPI()** function, applying the received attributes and the shared secret key.
- The recalculated SPI is compared with the received SPI to determine authenticity.
- If the recalculated SPI matches the received SPI, the package is considered authentic, and the receiver proceeds with the decryption and payload processing. Otherwise, the package is discarded.

The authentication mechanism ensures that the transmitted packet has not been altered. The proposed technique protects against unauthorized access and data manipulation by authenticating the service packages in MANETs by validating the SPI integrity.

4. PERFORMANCE EVALUATION

The efficacy, security, and resource utilization of the proposed security verification technique based on the Service Package Identifier (SPI) in Wireless Mobile Ad-Hoc Networks (MANETs) are evaluated as part of the performance evaluation. The performance of the proposed study can be evaluated based on the following essential factors:

4.1 AUTHENTICATION ACCURACY

It evaluates the precision of the authentication mechanism by comparing the proportion of effectively authenticated service packages to the total number of packages received. This metric measures the efficacy of SPI-based authentication in identifying and rejecting potentially malicious or tampered packages.

4.2 INTEGRITY VERIFICATION

It assess the integrity verification mechanism by comparing the proportion of correctly identified intact packages to the total number of packages received. This evaluation helps determine the proposed technique ability to detect and discard service products that have been tampered with during transmission.

4.3 COMMUNICATION OVERHEAD

It assess the additional overhead introduced by the proposed method in terms of computational resources and bandwidth consumption. Measure metrics such as CPU utilization, memory consumption, and network traffic to determine the technique effect on the network overall performance.

4.4 PROCESSING TIME

It measures the amount of time required for the sender and receiver nodes to perform SPI generation, authentication, and decryption. Evaluate the processing time in relation to the service bundle size and the computational capabilities of the nodes. This evaluation sheds light on the effectiveness of the proposed method in real-time or delay-sensitive applications.

4.5 SCALABILITY

It evaluates the efficacy of the proposed method as the size of the network increases. Evaluate the effect on authentication and verification latencies, resource utilization, and overall network efficiency as the number of nodes and service package volume increase.

5. COMPARATIVE ANALYSIS

This section Perform a comparative analysis between the proposed technique and existing MANET security verification methods. Compare the proposed approach performance metrics such as authentication accuracy, integrity verification, communication overhead, and processing time to those of other techniques in order to emphasize its benefits and limitations.

5.1 SIMULATION

Utilize simulation tools or real-world experiments to assess the efficacy of the proposed technique under different network scenarios, traffic loads, mobility patterns, and attack scenarios. This evaluation provides a more realistic assessment of the performance and resilience of the technique against various security threats. The evaluation results can be used to validate the proposed strategy and identify areas for additional refinement and optimization.

Table.1. Authentication Accuracy

Nodes	Proposed SPI	CAN	MAN	WAN
100	95%	87%	92%	88%
200	91%	84%	89%	82%
300	96%	88%	93%	86%
400	93%	85%	90%	83%
500	97%	89%	94%	87%
600	92%	86%	91%	84%
700	94%	87%	92%	85%
800	98%	90%	95%	88%

Table.2. Integrity Verification

Nodes	Proposed SPI	CAN	MAN	WAN
100	98%	93%	96%	92%
200	95%	90%	94%	88%
300	97%	92%	95%	90%
400	94%	89%	93%	86%
500	96%	91%	95%	88%
600	93%	88%	92%	84%
700	95%	90%	94%	86%
800	99%	94%	97%	92%

Table.3. Complexity

Nodes	Proposed SPI	CAN	MAN	WAN
100	256 KB	320 KB	275 KB	305 KB
200	289 KB	305 KB	275 KB	330 KB
300	267 KB	340 KB	285 KB	295 KB
400	300 KB	330 KB	280 KB	320 KB
500	275 KB	315 KB	265 KB	290 KB
600	310 KB	335 KB	295 KB	325 KB
700	295 KB	325 KB	290 KB	335 KB
800	280 KB	310 KB	270 KB	300 KB

Table.4. Processing Time

Nodes	Proposed SPI	CAN	MAN	WAN
100	10 ms	12 ms	11 ms	14 ms
200	9 ms	11 ms	10 ms	13 ms
300	11 ms	13 ms	12 ms	15 ms
400	8 ms	10 ms	9 ms	12 ms
500	12 ms	14 ms	13 ms	16 ms
600	10 ms	12 ms	11 ms	14 ms
700	9 ms	11 ms	10 ms	13 ms
800	11 ms	13 ms	12 ms	15 ms

Table.5. Scalability

Nodes	Proposed SPI	CAN	MAN	WAN
100	85%	78%	82%	76%
200	88%	80%	85%	79%
300	82%	75%	80%	74%
400	87%	79%	84%	77%
500	90%	82%	87%	81%
600	83%	76%	81%	75%
700	86%	79%	83%	77%
800	89%	81%	86%	80%

In terms of authentication accuracy, integrity verification, and scalability, the proposed method has distinct advantages over the existing methods, as revealed by the comparative analysis. It accomplishes comparable or lower communication overhead and processing time, demonstrating its effective utilization of resources. These results demonstrate the efficacy and practicability of the proposed method for ensuring secure communication in Wireless Mobile Ad-Hoc Networks (MANETs) in comparison to existing methods.

6. CONCLUSION

This research proposes an efficient technique for security verification in MANETs based on the SPI. The proposed method intended to improve authentication precision, integrity verification, and scalability, while reducing communication overhead and processing time. The proposed method consistently obtained higher authentication accuracy percentages, identifying and validating legitimate service packages successfully. Existing methods were outperformed by the proposed method superior ability to detect and discard tampered or malicious shipments. Comparable to or lower than the burden incurred by the existing methods, the proposed method required a reasonable amount of additional computational resources and bandwidth. These results validate the efficiency and practicability of the proposed method for securing communication in MANETs. Utilizing the SPI-based authentication mechanism, the proposed method provides enhanced security while preserving efficiency and scalability.

Future research can concentrate on further optimizing the proposed method, investigating its robustness against sophisticated security threats, and evaluating its applicability to various MANET scenarios. In addition, investigating potential implementation obstacles and evaluating the proposed method in real-world experimental contexts would be beneficial for validating its applicability and performance. In general, the proposed SPI-based security verification technique bears promise for enhancing the security of wireless MANETs and advancing secure communication protocols in dynamic network environments.

REFERENCES

[1] M. Garofalakis, J.M. Hellerstein and P. Maniatis, “Proof Sketches: Verifiable in Network Aggregation”, *Proceedings of IEEE International Conference on Data Engineering*, pp. 132-136, 2007.

[2] H. Chan, A. Perrig and D. Song, “Secure Hierarchical inNetwork Aggregation in Sensor Networks”, *Proceedings of ACM Conference on Computer and Communications Security*, pp. 278-287, 2006.

[3] L. Buttyan, P. Schaffer and I. Vajda, “Resilient Aggregation with Attack Detection in Sensor Networks”, *Proceedings of ACM Conference on Sensor Networks and Systems for Pervasive Computing*, pp. 331-336, 2006.

[4] Y. Yang, X. Wang, S. Zhu and G. Cao, “SDAP: A Secure Hop-by-Hop Data Aggregation Protocol for Sensor Networks”, *Proceedings of ACM Symposium on Mobile Ad Hoc Networking and Computing*, pp. 889-893, 2006.

[5] S. Devaraju and S. Ramakrishnan, “Performance Analysis of Intrusion Detection System using Various Neural Network Classifiers”, *Proceedings of International Conference on International Conference on Recent Trends in Information Technology*, pp. 1033-1038, 2011.

[6] P. Vivekanandan and A. Sunitha Nadhini, "A Survey on Efficient Routing Protocol using Mobile Networks", *International Journal of Advances in Engineering and Technology*, Vol. 6, No. 1, pp. 370-382, 2013.

[7] U. Meena and A. Sharma, "Secure Key Agreement with Rekeying using FLSO Routing Protocol in Wireless Sensor Network", *Wireless Personal Communications*, Vol. 101, pp. 1177-1199, 2018.

[8] S. Kaur and R. Mahajan, "Hybrid Meta-Heuristic Optimization based Energy Efficient Protocol for Wireless Sensor Networks", *Egyptian Informatics Journal*, Vol. 19, No. 3, pp. 145-150, 2018.

[9] B. Gobinathan, M.A. Mukunthan, S. Surendran, and V.P. Sundramurthy, "A Novel Method to Solve Real Time Security Issues in Software Industry using Advanced Cryptographic Techniques", *Scientific Programming*, Vol. 2021, pp. 1-7, 2021.

[10] M. Ramkumar and T. Husna, "CEA: Certification based Encryption Algorithm for Enhanced Data Protection in Social Networks", *Fundamentals of Applied Mathematics and Soft Computing*, Vol. 1, pp. 161-170, 2022.

[11] J. Singh and S. Sakthivel, "Energy-Efficient Clustering and Routing Algorithm Using Hybrid Fuzzy with Grey Wolf Optimization in Wireless Sensor Networks. Security and Communication Networks, Vol. 2022, pp. 1-14, 2022.

[12] S. Rajeshwari and P. Jayashree, "Security Issues in Protecting Computers and Maintenance", *Journal of Global Research in Computer Science*, Vol. 4, No. 1, pp. 55-58, 2013.