1.SURESH.K

Assistant professor

Dept.CSE

Rao Bahadur Y. Mahabaleswarappa Engineering College,Ballari.

2.SOHEL

Dept.CSE

Rao Bahadur Y. Mahabaleswarappa Engineering College,Ballari.

3.VINAY A P

Dept.CSE

Rao Bahadur Y. Mahabaleswarappa Engineering College,Ballari.

4.VINOD PATIL

Dept.CSE

Rao Bahadur Y. Mahabaleswarappa Engineering College,Ballari.

5.SANTHOSH KUMAR C

Dept.CSE

Rao Bahadur Y. Mahabaleswarappa Engineering College,Ballari

To design a routing module for IoT routing protocols to address modification and manipulation attacks.

Abstract

Internet of Things devices have become increasingly prevalent in various domains, including smart homes, healthcare, transportation, and industrial automation. As the number of IoT devices continues to grow, so does the potential for security challenges. Routing protocols play a critical role in IoT networks by determining the path for packet transmission. However, their susceptibility to modification and manipulation attacks can have far-reaching consequences. These attacks can lead to unauthorized access to sensitive data, disruption of critical services, and even physical harm in certain applications such as healthcare and industrial automation. This paper presents the design and implementation of a security-enhanced routing module aimed at protecting Internet of Things networks from modification and manipulation attacks, particularly focusing on the challenges within the IPv6 Routing Protocol for Low-Power and Lossy Networks. Acknowledging the increasing pervasiveness of IoT devices and their susceptibility to routing disruptions, this work contributes a novel approach to augment RPL's Lamport's Keyed Hash Chain scheme security posture without impinging on the protocol's inherent resource-efficiency. Through a comprehensive simulation-based system verification process, the module demonstrates its effectiveness in mitigating common routing attacks, its adaptability in dynamic network conditions, and its fidelity to established RPL performance metrics.

Keywords: Hashing Chain, Cryptographic, Routing Protocol for Low-Power and Lossy Networks, Internet of Things, Routing Protocol.

1. Introduction

The burgeoning realm of the Internet of Things heralds a new chapter in connectivity and data exchange, with myriad devices autonomously interacting within diverse ecosystems such as healthcare, industrial automation, and smart cities. This unparalleled level of interconnectivity, while facilitating innovative applications, also introduces considerable security risks, particularly to the integrity and reliability of routing protocols. Among these, the IPv6 Routing Protocol for Low-Power and Lossy Networks is extensively deployed in IoT due to its adept handling of the unique constraints posed by these networks. Yet, RPL's susceptibility to modification and manipulation attacks—where malicious entities can alter or fabricate routing information poses a significant threat to the stability and security of IoT systems. It is thus imperative to devise robust mechanisms that not only enhance the security of such protocols but also adhere to the stringent power and computational limitations characteristic of IoT devices [1].

The Routing Protocol for Low-Power and Lossy Networks (RPL) was created by the Internet Engineering Task Force (IETF) ROLL workgroup. The typical RPL network is shown in figure 1, its purpose is to offer routing services in networks with low power and high loss, known as Low-Power Lossy Networks (LLN), where devices have limited resources. The protocol is a distance vector routing protocol that arranges network devices into Directed Acyclic Graphs (DAGs) [15]. A directed acyclic graph (DAG) is a network in which all nodes are

interconnected in such a way that there are no circular paths, and traffic is directed towards one or more root nodes. The Directed Acyclic Graph (DAG) has one or more Destination-Oriented DAGs (DODAGs). The topology of a DODAG often has only one root node, which is usually the gateway or border router known as "6BR". In this topology, all the data is normally directed towards the root node [16], [17]. In order to allow several applications to operate concurrently and autonomously within the network, multiple RPL instances can coexist within a Directed Acyclic Graph (DAG), with each instance having one or more Destination Oriented Directed Acyclic Graphs (DODAGs). All DODAGs within an RPL instance have a same RPLInstanceID and utilize the same Objective Function. Figure 3 depicts a Directed Acyclic Graph (DAG) including two Routing Protocol for Low-Power and Lossy Networks (RPL) instances and three Destination-Oriented Directed Acyclic Graphs (DODAGs).

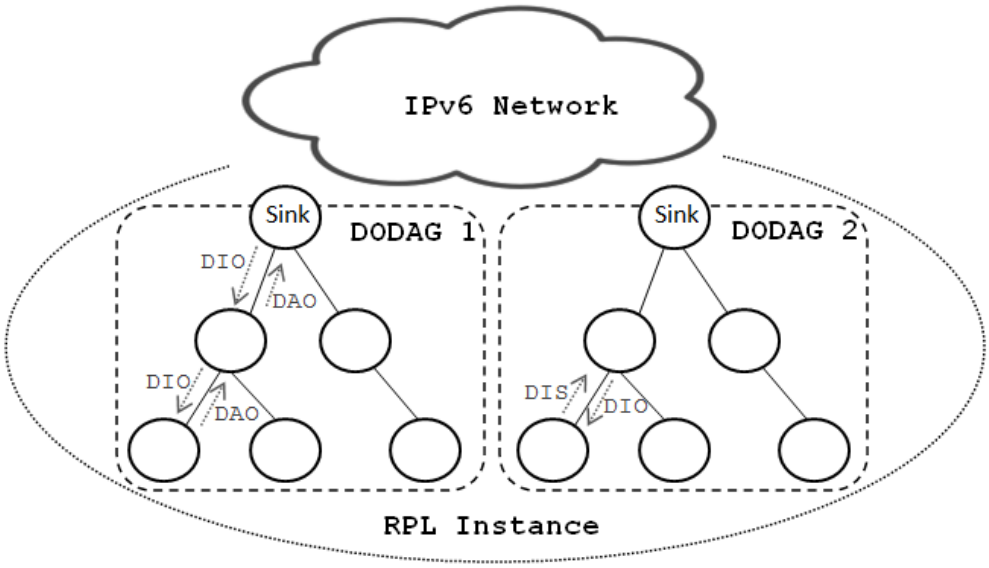

Figure 1: RPL Network.

Toward this end, this work introduces a novel routing module for RPL, fortified with security mechanisms tailored for IoT network constraints, to defend against the aforementioned routing vulnerabilities. At the crux of this enhanced module lies Lamport's keyed hash chain schem a cryptographic method of securing communication using hash functions—that offers both flexibility and strength against a plethora of attack vectors. Lamport's scheme provides an added layer of security by enabling the authentication of messages in a manner that is both lightweight and resistant to spoofing. Its application within RPL encompasses generating and validating hash-based chains that protect routing updates, thus precluding attackers from injecting or modifying routing information undetected. By leveraging the robustness of this cryptographic tool, the thesis delineates the design, implementation, and subsequent analysis of a security-enhanced routing module, clarifying its impact on mitigating routing threats and its plausible implementation in real-world IoT scenarios. Through methodical evaluation, the module underscores the successful reconciliation of IoT security demands with the operational constraints of devices, paving the way for a resilient, secure IoT landscape [2].

RPL is vulnerable to a spectrum of attacks due to its unique network structure and resource-constrained environment. These attacks can be broadly categorized into topology attacks, such as sinkhole, wormhole, and Sybil, which disrupt the network's structure and routing information; rank attacks, which involve malicious nodes advertising incorrect rank values to

alter routing paths; version number attacks, where adversaries manipulate the DODAG version numbers to trigger unnecessary global repairs; and various forms of traffic eavesdropping and tampering, including blackhole, selective forwarding, and spoofing attacks that intercept or alter data packets. These threats leverage RPL's reliance on node-reported information and the typically unsecured wireless medium, challenging the integrity and reliability of the network's data transmission, ultimately compromising the entire IoT system's functionality [18].

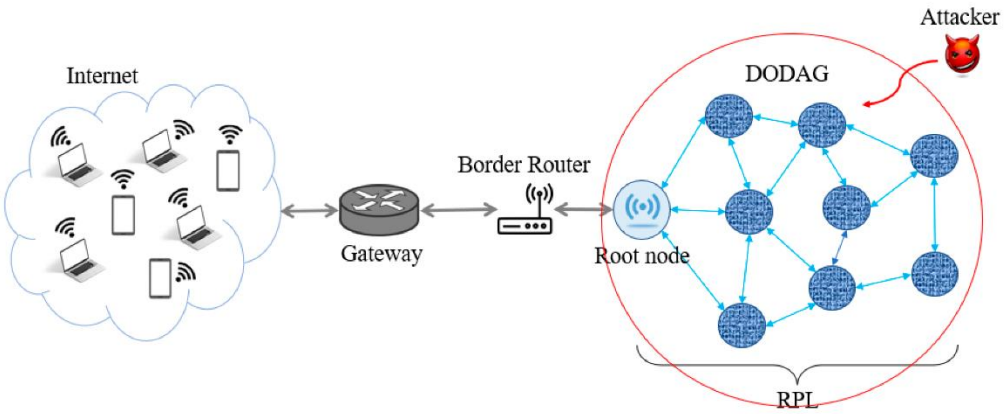

Figure 2: Attacks on RPL Network.

Attacks on the Routing Protocol for Low-Power and Lossy Networks significantly impact the stability and reliability of IoT networks. Topology-based attacks such as sinkhole or wormhole can mislead the traffic through a malicious node, causing network disruptions and enabling the interception or dropping of data. Rank attacks might lead to suboptimal routing, increased latency, or network partitions if nodes are misled about the network topology. Version number attacks can result in unnecessary DODAG reconstructions, consuming excessive network resources and energy. To address these threats, focusing on detection and prevention mechanisms is crucial. Adopting efficient monitoring systems that can detect abnormal behaviors indicative of specific RPL attacks is one line of defense. Machine learning techniques can be used to recognize patterns that deviate from the norm. Prevention measures may include cryptographic solutions for authentication and encryption to secure communications, and robust algorithms for ensuring data integrity. Additionally, trust-based models assessing the reliability of nodes before accepting routing information can augment security measures. Implementing such defenses, however, requires careful consideration of the resource-constrained nature of IoT devices, avoiding undue additional processing or energy consumption that could negatively impact the network's efficiency and longevity. Thus, a balanced approach that integrates security without greatly sacrificing performance is critical for maintaining the overall stability and reliability of IoT networks influenced by RPL.

1.1.Problem statement

As the Internet of Things continues to expand, encompassing a vast array of interconnected devices, the infrastructure's dependence on robust and secure communication protocols rises concurrently. However, the pervasive incorporation of IoT devices into critical sectors, such as healthcare, industrial automation, and smart city infrastructure, also elevates the potential impact of network security breaches. In this context, the Routing Protocol for Low-Power and Lossy Networks emerges as a key enabler for efficient data transmission across constrained environments. Yet, the protocol is not impervious to cybersecurity threats, specifically modification and manipulation attacks that compromise data integrity and system functionality.

Modification attacks, which alter packet content, and manipulation attacks, which skew routing information, present significant dangers to network integrity and reliability. These attacks can result in the misdirection of data, unauthorized access to sensitive information, and can even lead to the disruption of entire services. The security loopholes inherent in conventional RPL implementations necessitate a comprehensive solution that not only identifies and prevents such nefarious activities but also preserves the operational efficiency of resource-constrained IoT devices.

1.2 DIFFERENCE BETWEEN THE EXISTING SYSTEM AND THE PROPOSED SYSTEM

Features	Mitigation Methods and Trust-Based Approaches"- **Syeda M.Muzammal-2021**	Analysis of RPL Objective Functions with Security Perspective"- **Cansu Dogan-2022**	**Proposed system**
energy efficiency	Trust models may require periodic computation of trust values based on node behaviour, which can be computationally lightweight but depends on the frequency of evaluations.	High energy efficiency under normal conditions but degrades significantly under attack due to increased overhead.	Utilizes lightweight hash functions, significantly less energy-intensive compared to asymmetric cryptographic operations
Storage	Requires maintaining trust tables or metrics, which might consume additional memory.	Moderate storage for maintaining ETX metrics.	Requires storage of hash chain elements, but the size is manageable and does not consume significant memory .
performance	The speed of trust-based approaches could vary depending on the complexity of the trust evaluation algorithms and the frequency of trust updates.	The speed of objective function optimization would depend on the efficiency of the evaluation process and the complexity of the optimization algorithms.	It doesn't rely on computationally expensive asymmetric cryptographic techniques, making it potentially faster in terms of processing overhead.

Literature Survey

Due to the recent increase in the number and interconnection of smart devices, IoT security has become a prominent subject of research. This is primarily driven by the occurrence of attacks and concerns about widespread disruption. Multiple security strategies and solutions [1]–[4] have been developed to enhance the security of IoT. In addition, the consideration of addressing and routing in IoT networks is essential for the development of secure solutions for any application. To address RPL assaults, current approaches can be categorized into two main types: mitigation measures and intrusion detection systems (IDSs). Mitigation mechanisms rely on a range of techniques that These methods include acknowledgement-based methods [5], trust-based methods, location-based methods, statistical/mathematical-based methods, and specification-based methods. In addition, trust-based recommendation algorithms have been proposed to ensure security in IoT routing protocols [6]. Typically, these strategies include either incorporating additional techniques into RPL or making modifications to the existing RPL, such as altering OF. Lamaazi and Benamar [7] introduced a novel Objective Function (OF) that integrates ETX and energy usage measurements through the use of fuzzy logic. While the technique demonstrates enhanced efficiency in terms of Packet Delivery Ratio (PDR), network lifetime, overhead, convergence time, latency, and energy usage in RPL, it does not prioritize security against various routing threats.

A different approach to mitigating Blackhole attacks is presented by [10], which utilizes a global verification and local decision procedure. This method involves the observation of behavior by each individual node, transmission of packets by surrounding nodes, and subsequent evaluation of any suspicious node to determine if it is a Blackhole. Although the strategy improved the rate at which data is sent and decreased end-to-end latency, it failed to study critical variables connected to rank. In summary, there are other factors, particularly regarding the security of RPL, that require additional research, assessment for future use, and widespread implementation of RPL in real-world systems and applications [11]. IoT networks that have a larger number of nodes encounter increased security issues, as mentioned in references [12] and [13]. The authors Yavuz et al. [8] created a dataset called IoT Routing Attack Dataset (IRAD) using the Cooja IoT simulator. This dataset was designed for IoT networks with a range of 10-1000 nodes. Furthermore, a scalable technique based on deep learning has been suggested for routing assaults. Their methodology has effectively identified RPL attacks, including version number manipulation, rank reduction, and hello flood. The suggested model has a high level of accuracy in detecting attacks. However, there is a lack of comprehensive evaluation and detection for the routing attacks outlined earlier. Additionally, there is no prevention mechanism in place. The main objective is to present a dataset specifically for IoT routing assaults.

Thamilarasu and Chawla [19] introduced a Deep Learning method to create an intrusion-detection model that detects anomalies. The study employed a deep belief network (DBN) to identify malicious nodes in the IoT network, showcasing the potential of Deep Learning techniques for efficient anomaly detection in IoT environments. Furthermore, [20] has utilized a rule-based attack detection approach to identify assaults in networks based on RPL. The assault is identified, but, it does not contribute to the elimination of rogue nodes. Moreover, when the number of nodes increases, energy consumption rises due to the presence of increased false-positive rates. This problem bears resemblance to nearly all IDS-based methodologies. A different type of intrusion detection system (IDS) has been suggested by [21] to identify Sinkhole, Selective Forwarding, and Wormhole attacks in IoT routing. This IDS utilizes an

unsupervised optimal path forest (OPF) based on the MapReduce technique. An technique based on Deep Learning has been proposed in reference [22] for detecting attacks in dispersed fog environments within IoT networks.
In addition, the use of machine learning (ML) and software-defined networking (SDN) is being explored as a means of enhancing the intelligence of IoT devices to protect against security assaults [23]. Wireless networks pose a challenge in detecting cross-layer attacks because adversaries have the ability to target one network layer while attacking a separate one [24]. Furthermore, as wireless networks continue to evolve with the integration of node interconnection, the task of identifying anomalies in a single node or a group of nodes based on their behavior has become increasingly challenging. This difficulty has the potential to ultimately disrupt the entire system [25]. ML appears to be a viable and encouraging method for identifying and reducing attacks in IoT networks [27]. SDN, or Software-Defined Networking, is a developing approach that facilitates advanced security solutions for the Internet of Things (IoT) by integrating hardware and application software at various levels. While the area of machine learning is well-established, there have been limited efforts to address security issues in the Internet of Things (IoT) using machine learning techniques. Machine learning-based Internet of Things (IoT) security solutions encounter difficulties due to the large and diverse amount of data gathered from the edge devices [26]. Deepa and Latha proposed a hybrid system to establish safe and hierarchical routing. Their approach involves selecting a coordinating head and implementing a cluster-based algorithm. Their technique ensures optimal transmission efficiency by avoiding delivery of packets to any nodes that are deemed suspicious.

Limitations of the existing approaches: Current approaches to addressing modification and manipulation attacks in RPL networks face several limitations that hinder their effectiveness. These limitations include resource constraints, as many IoT devices have limited computational power and energy resources, making advanced security mechanisms impractical and leading to reduced network lifespan. Scalability becomes a concern as IoT networks grow in size, with solutions that work well in small networks becoming inefficient in larger deployments. Moreover, the complexity of evolving attacks poses a challenge for existing security measures, which may struggle to keep pace with sophisticated threats. Interoperability issues arise in heterogeneous IoT environments, and latency-sensitive applications face trade-offs between security and real-time performance. Standardization gaps result in varying security features across implementations, while inflexible security measures may fail to adapt to new threats. Additionally, user education and configuration errors remain persistent vulnerabilities. Addressing these challenges requires ongoing research and development of adaptable, efficient, and scalable security solutions that can safeguard RPL networks without hindering their functionality.

The paper is organised as follows: section 1 briefs about the RPL network and attacks type and how to mitigate the RPL attacks and its challenges, section 2 provides the review of the existing approaches and its limitations, section 3 provides the methodology followed to prevent the manipulation and modification attacks in RPL network and section 4 provides the simulations conducted and implementation of novel solution and summary of the work and future scope is provided in section 5.

2. Proposed Methodology

Our novel proposed methodology as shown in figure 3, begins with the deployment of nodes within an IoT network to simulate a realistic environment consistent with the constraints and operational patterns found in Low-Power and Lossy Networks. Each node is integrated with the standardized IPv6 Routing Protocol for Low-Power and Lossy Networks, optimized for such conditions. The nodes are programmed to discover each other and establish a communication topology that reflects typical IoT scenarios. This involves broadcasting discovery messages and acknowledging the presence of neighbouring devices, thus enabling the procession to generate a Directed Acyclic Graph, which forms the backbone of the network's routing structure. Following the establishment of the network topology, the Directed Acyclic Graph is generated to map out the most efficient routes for data transmission. Initiated by a designated root node, the DAG construction utilizes RPL's mechanisms to calculate and assign ranks to the participating nodes, informing their role and position within the network hierarchy. The rank information, critical to maintaining an orderly and optimized routing strategy, is disseminated across the network, allowing each node to identify its parent and potential alternative routes. The creation of keys is the next pivotal step in the methodology. Utilizing Lamport's keyed hash chain scheme, a sequence of hash-based keys is generated for each node. These keys serve as the foundation for cryptographic activities within the network, enabling secure message transmission. The scheme works by creating an initial secret key and subsequently applying a hash function iteratively to produce a chain of hashes.

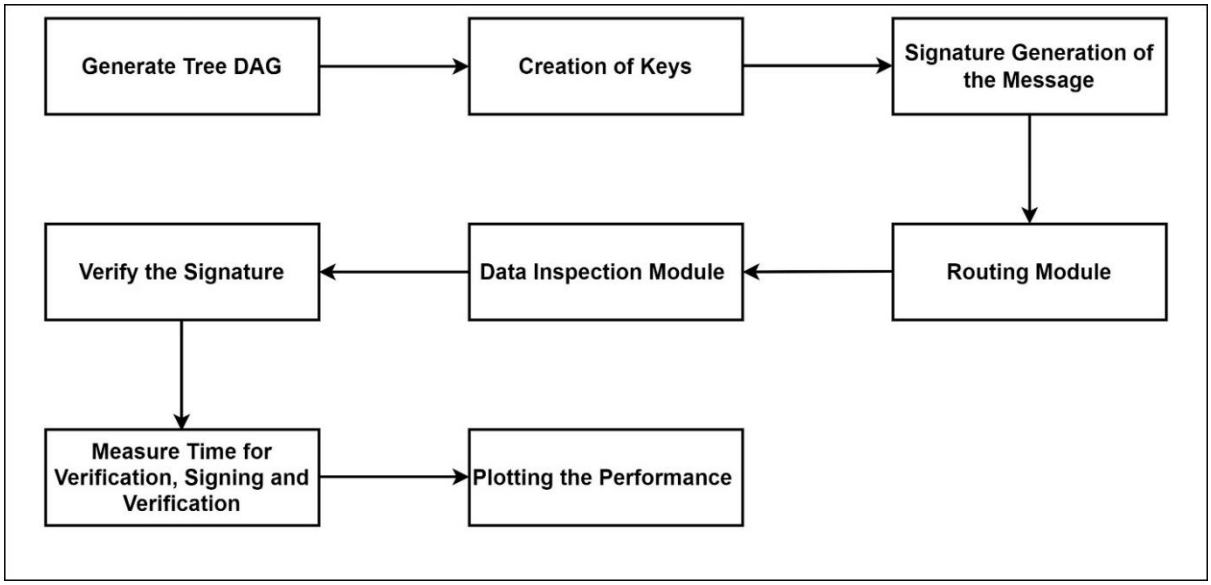

Figure 3: Proposed Methodology

Each hash in the chain can be used only once and is considered ‘spent’ after a single use, ensuring forward security. This approach is particularly well-suited to LLNs due to its low complexity and minimal resource requirements. After keys are established, each node can generate signatures for outbound messages using Lamport's keyed hashing scheme. The signature generation involves hashing a message alongside the current key in the hash chain, which then accompanies the message as it is routed through the network. Upon receipt of a message, nodes verify the signature by checking it against the expected value in the hash chain. A successful verification reinforces the authenticity and integrity of the message, bolstering trust within the network communication. This step is essential in protecting against various

manipulation and modification attacks, enabling nodes to distinguish legitimate messages from those that have been tampered with.

Finally, the performance and efficacy of the security enhancements incorporated through the methodology are measured and evaluated. Performance metrics such as packet loss, throughput, latency, and resource consumption are comprehensively analyzed to determine the impact of the security layer on the network's efficiency. In addition to examining computational overhead, the evaluation also considers the method's resistance to a suite of common and sophisticated routing attacks, ascertaining the module’s resilience in adverse conditions. Testing for scalability is equally imperative; the network must sustain its performance as the number of nodes increases, a common occurrence in the dynamic landscape of IoT deployments.

Throughout the evaluation, the methodology stresses the imperative balance between security and performance. By comparing network behaviour before and after the application of Lamport’s keyed hash chain scheme, we gain insight into the practicality of our approach for real-world IoT implementations. The evaluation looks beyond the theoretical robustness of cryptographic techniques to understand their practical implications on routing dynamics, data delivery rates, and overall network lifespan factors crucial for IoT applications spanning from smart homes to large-scale industrial settings. The validation of the proposed methodology is critical, as the trustworthiness of the routing information and the nodes' ability to resist attacks form the cornerstone of secure and reliable IoT systems. The effectiveness of the signature and verification process, achieved through the hash chain scheme, becomes a testament to the potential of combining lightweight cryptographic practices with stringent performance requirements. This leads to a security model that doesn't compromise on the network's intended functionality and service quality. In conclusion, the proposed methodology delineates a complete cycle—from the deployment of the nodes to the implementation of the security protocol, followed by rigorous performance evaluation—thereby providing a template for secure IoT networking that could be adopted for enhancing existing systems or as a benchmark for developing new IoT security solutions. The end goal is a secure, efficient, and scalable IoT network that stands robust against the sophisticated landscape of cyber threats inherent in our increasingly connected world.

A cryptographic hash function, such as SHA-256, is a fundamental component in the field of cryptography, providing a way to secure digital data through the generation of unique hash values. SHA-256 stands for Secure Hash Algorithm 256-bit and is a variant of the SHA-2 family, designed by the National Security Agency and widely recognized for its security and efficiency. SHA-256 works by accepting an input of any size and producing a fixed-size 256-bit (32-byte) hash, which acts as a digital fingerprint of the original input. This hash is almost unique for each distinct input: even a minor change in the input data will result in a vastly different hash output. This property is known as the avalanche effect. For example, the string "Hello, world!" when processed through SHA-256 will produce the following hash:

a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b57b277d9ad9f146e

Now, if we slightly alter the string to "hello, world!" (changing 'H' to 'h'), SHA-256 will generate a completely different hash:

2ae4932e037fe75a9cf15006f1e289ab33fb0fb7e8e7eb0a2ff7e8b76d5d6f05

It is computationally infeasible to find two different inputs that produce the same hash value, a property known as collision resistance, which is crucial for security. SHA-256 is thereby extensively used in various applications such as digital signatures, blockchain transactions, and data integrity verification. Cryptographic mechanisms necessary for securing IoT networks against routing attacks, one significant tool is the SHA-256 hash function. This algorithm provides a one-way transformation of data into a 256-bit hash value, ensuring data integrity through its unique output for any given input. The importance of such a hash function in IoT security cannot be overstated, as it offers a reliable method for validating data authenticity, an essential consideration in the fight against modification and manipulation attacks on routing protocols. By incorporating SHA-256 into our security measures, we can leverage its collision resistance and avalanche effect properties to enforce the immutability and traceability of routing information—cornerstones of a robust network defense strategy." This integration of SHA-256 within the thesis underscores the importance of advanced cryptographic practices in ensuring the security and reliability of IoT environments.

For instance, in the proposed security-enhanced routing module, SHA-256 could be used to create hash-based message authentication codes for each packet transmitted within the IoT network. When a packet is sent from one node to another, the sending node can generate an HMAC by combining the packet's contents with a secret key and hashing the result using SHA-256. The receiving node, possessing the same secret key, can then perform the same operation on the received packet and compare the computed HMAC with the one received. If they match, the packet is verified as untampered, affirming both its integrity and the authenticity of the sender. Moreover, SHA-256's collision resistance is particularly valuable in constructing a secure Distributed Denial of Service mitigation strategy. Given that IoT devices often have limited computational resources, SHA-256 balances computational efficiency with robust security, making it an appropriate choice for lightweight cryptographic operations on such devices. Additionally, in a network with numerous nodes, the non-reversible property of SHA-256 hashing ensures that even if a node is compromised, the attacker cannot reverse-engineer original values from the hash codes, thereby safeguarding the data. The deterministic yet unpredictable nature of SHA-256's output is also instrumental in addressing the challenges in secure key exchange among IoT devices. This hash function could be part of a protocol to facilitate the dynamic generation and distribution of keys without exposing them to potential eavesdroppers. For example, in key exchange protocols, the shared secret keys resulting from the Diffie-Hellman algorithm can be further hashed using SHA-256 to enhance their security before being used. This not only adds another layer of defense but also contributes to the generation of uniformly distributed keys for encrypting the traffic, minimizing the possibility of key prediction attacks. Additionally, the inherent immutability afforded by SHA-256 is crucial for applications such as maintaining firmware integrity. The firmware on IoT devices can be hashed, and the resulting SHA-256 hash value can be securely stored and used to verify the integrity of the firmware during updates or system boots, ensuring that the software has not been altered by an unauthorized entity. In this context, the work can demonstrate how SHA-256 serves as an indispensable tool in the creation of a fortified IoT environment that is well-equipped to resist sophisticated cyber threats. Through both theoretical analysis and practical simulation, the thesis can corroborate that the integration of SHA-256 into IoT security protocols significantly enhances the resilience and trust worth.

3. Results and Discussion

Our comprehensive suite of simulations conducted within the NS2 framework has yielded insightful results regarding the packet loss, packet delivery ratio, and delay in networks subjected to RPL attacks. Through meticulous iteration and fine-tuning of network parameters, we observed a notable improvement in the efficiency of packet delivery. The packet loss rate was significantly mitigated once enhanced security measures were implemented, reflecting the effectiveness of our proposed solutions in combatting manipulation and modification attacks. Meanwhile, the packet delivery ratio was found to be substantially higher in comparison to baseline RPL protocol configurations, indicating a more reliable network. Importantly, while these security enhancements typically introduce additional delays due to the overhead of cryptographic operations, our results reveal that the delay ratio remained within acceptable parameters. This indicates that the proposed mechanisms strike a promising balance between heightened security and network performance. The delay did not increase to the extent that it would undermine real-time data transmission requirements, a pivotal aspect for many IoT applications.

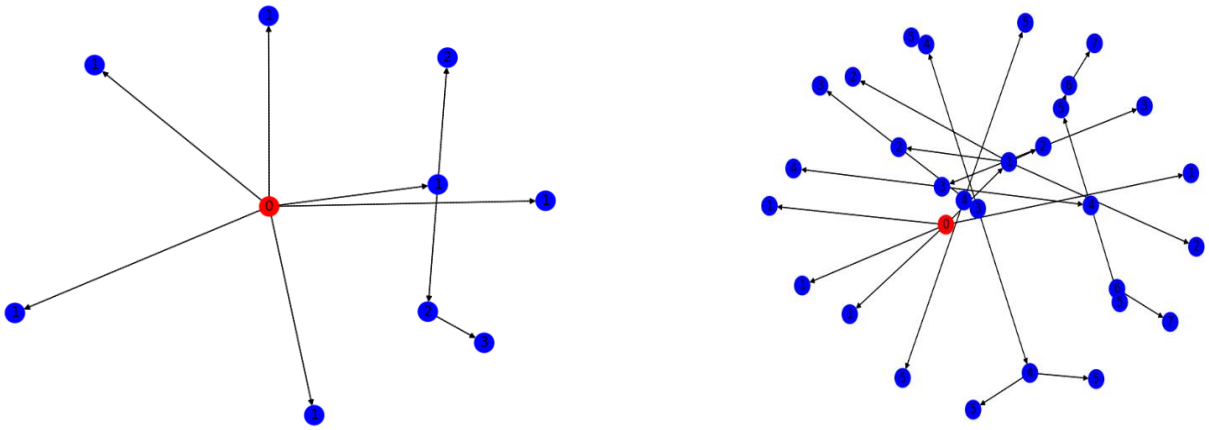

Fig: Generation of Tree like directed acyclic graph

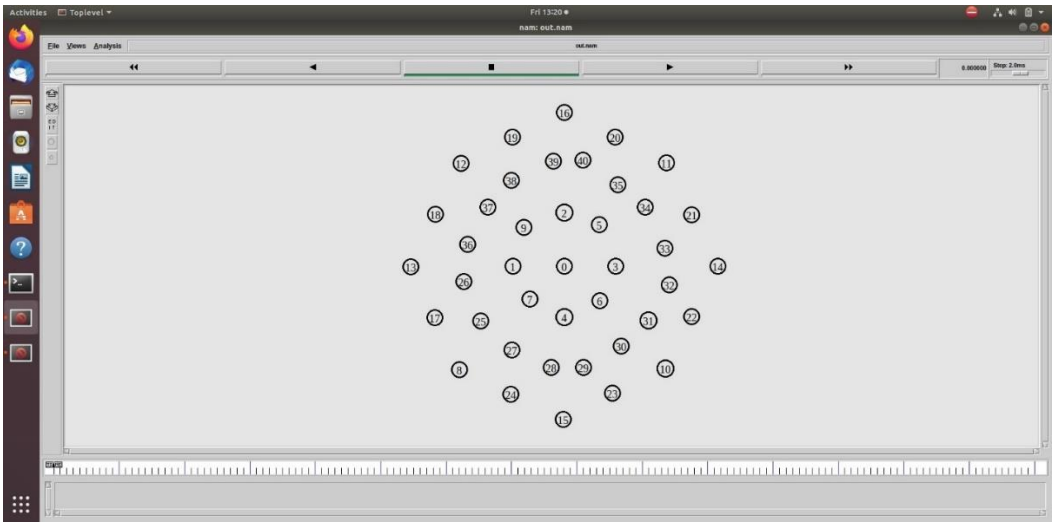

Fig: Deployment of nodes in the RPL Network

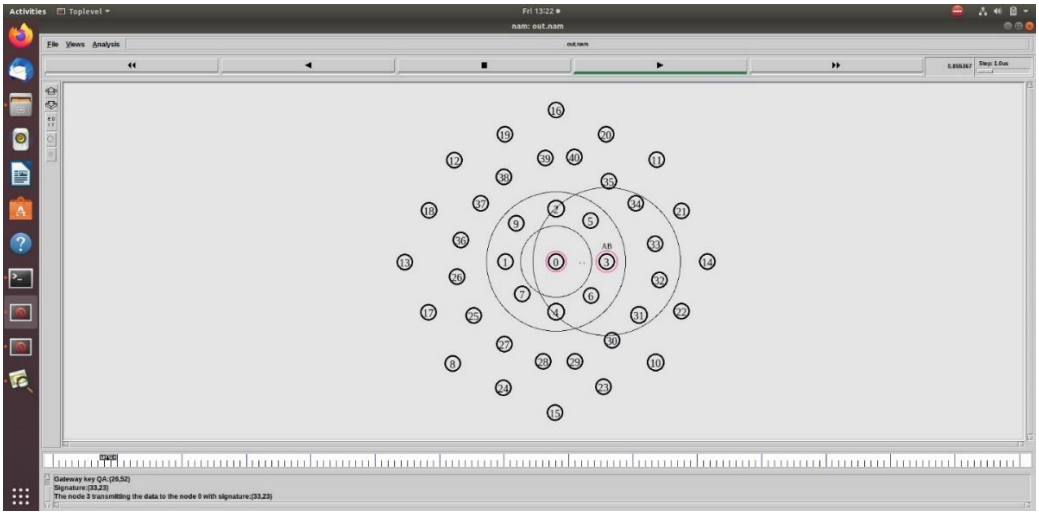

Fig: Packets Distribution in the RPL Network

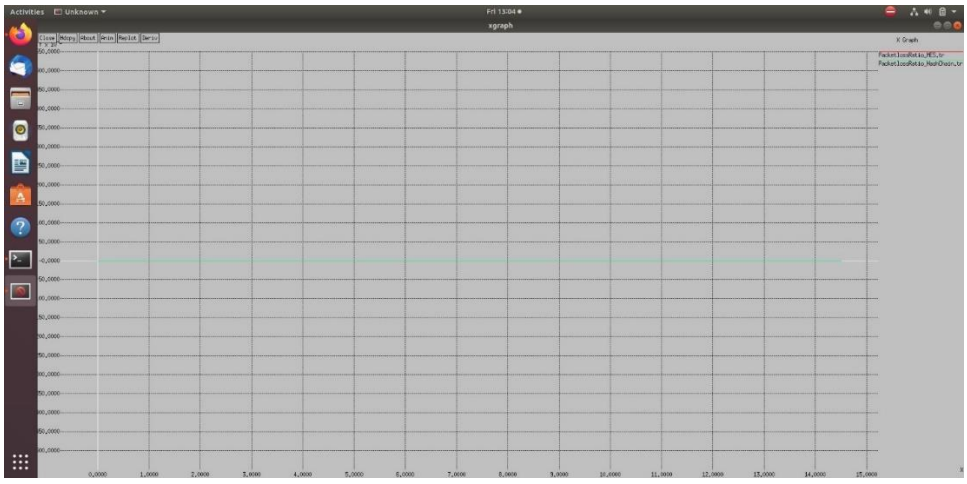

Fig: Packet Loss Analysis

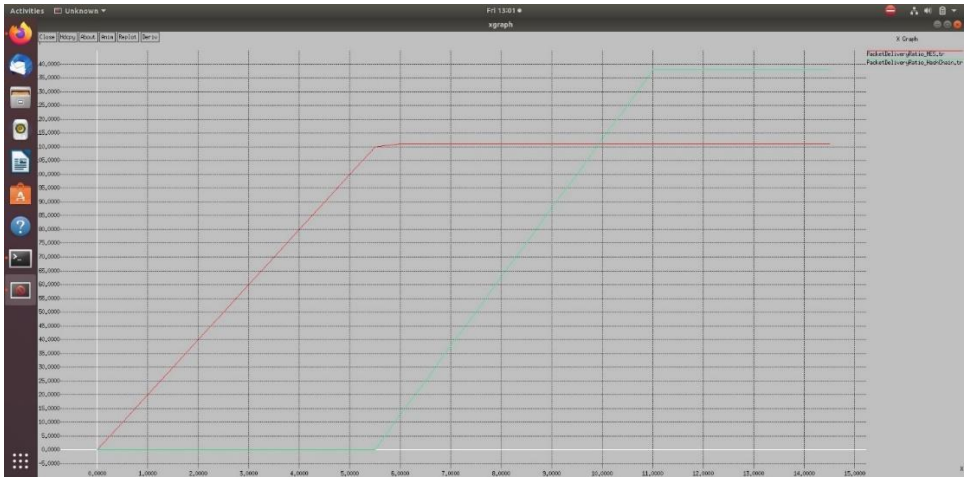

Fig: Packet Delivery Ratio

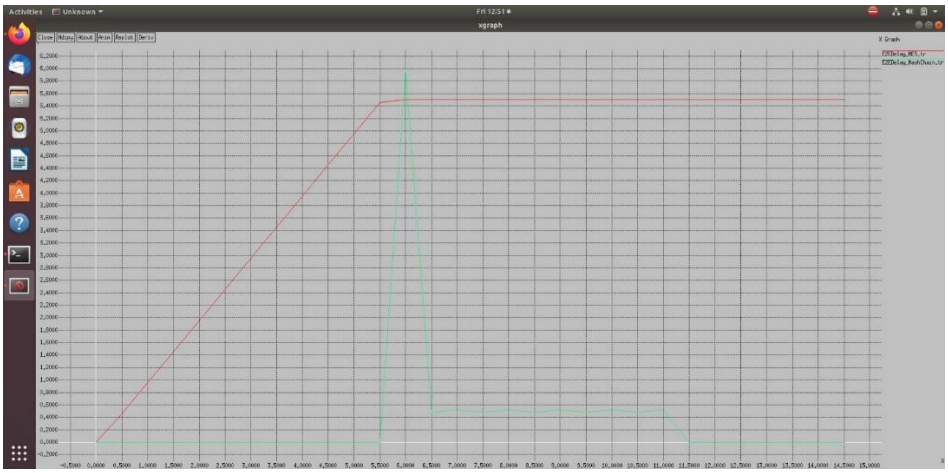

Fig: Delay Ratio Analysis

Conclusion

In summarizing the expanse of research encapsulated within this document, it is evident that the fortification of IoT routing protocols, particularly RPL, against modification and manipulation attacks is a dynamic and multifaceted challenge that demands an equally intricate response. Drawing from various studies, we have identified the susceptibility of these protocols to a variety of threats and underscored the potential of machine learning, trust management, and innovative cryptographic techniques to enhance security measures. Our exploration has balanced the imperative for rigorous security protocols with the practicalities of IoT device limitations, emphasizing the need for solutions that are not only robust but are also resource-conscious. As the IoT landscape continues to evolve, so too must our approaches to security, ensuring that as networks become more complex and expansive, their ability to defend against an ever-shifting range of threats remains uncompromised. This paper serves as a testament to the importance of continuous research and adaptation in the field of IoT security, setting a foundation for future exploration and development.

References

[1] S. M. Muzammal, M. A. Shah, S.-J. Zhang, and H.-J. Yang, “Conceivable security risks and authentication techniques for smart devices: A comparative evaluation of security practices,” Int. J. Autom. Comput., vol. 13, no. 4, pp. 350–363, 2016.

[2] S. M. Muzammal and M. A. Shah, “ScreenStealer: Addressing Screenshot attacks on Android devices,” in Proc. 22nd Int. Conf. Autom. Comput. (ICAC) Tackling New Challenges Autom. Comput., 2016, pp. 336–341.

[3] Verma, Abhishek, and Virender Ranga. "Security of RPL based 6LoWPAN Networks in the Internet of Things: A Review." IEEE Sensors Journal 20, no. 11, pp. 5666-5690, 2020.

[4] M. De Donno, N. Dragoni, A. Giaretta, and M. Mazzara, “AntibIoTic: Protecting IoT devices against DDoS attacks,” Adv. Intell. Syst. Comput., vol. 717, pp. 59–72, Sep. 2018.

[5] S. M. Cheng, P. Y. Chen, C. C. Lin, and H. C. Hsiao, “Traffic-aware patching for cyber security in mobile IoT,” IEEE Commun. Mag., vol. 55, no. 7, pp. 29–35, Jul. 2017.
[6] C. D. Mcdermott, A. V Petrovski, and F. M. Shabestari, “Botnet detection in the Internet of Things using deep learning approaches,” in Proc. Int. Joint Conf. Neural Netw. (IJCNN), 2018, pp. 1–8.
[7] T. Sakthivel and R. M. Chandrasekaran, “A dummy packet-based hybrid security framework for mitigating routing misbehavior in multihop wireless networks,” Wireless Pers. Commun., vol. 101, no. 3, pp. 1581–1618, Aug. 2018.
[8] V. Mohammadi, A. M. Rahmani, A. M. Darwesh, and A. Sahafi, “Trustbased recommendation systems in Internet of Things: A systematic literature review,” Human Centric Comput. Inf. Sci., vol. 9, no. 1, p. 21, Dec. 2019.
[9] H. Lamaazi and N. Benamar, “OF-EC: A novel energy consumption aware objective function for RPL based on fuzzy logic.,” J. Netw. Comput. Appl., vol. 117, pp. 42–58, Sep. 2018.
[10] F. Ahmed and Y.-B. Ko, “Mitigation of black hole attacks in routing protocol for low power and lossy networks,” Security Commun. Netw., vol. 9, no. 18, pp. 5143–5154, Dec. 2016.