International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 /doi:10.14445/22315381/IJETT-V69I10P217

Volume 69 Issue 10, 137-145, October, 2021
©2021 Seventh Sense Research Group®

An Efficient Authentication Technique to Protect IoT Networks from Impact of RPL Attacks

Smita Sanjay Ambarkar[1], Narendra Shekokar[2]

[1]*Research Scholar, Department of Computer Engineering, D.J.Sanghvi College of Engineering, Vile Parle, Mumbai, India*

[1]*Assistant Professor, Department of Computer engineering, LTCoE, Navi Mumbai, India*

[2]*Professor, Department of Computer Engineering, D.J.Sanghvi College of Engineering, Vile Parle, Mumbai, India*

[1]smita.ambarkar27@gmail.com, [2]narendra.shekokar@djsce.ac.in

Abstract *- The Internet of Things (IoT) changes the perspective of everyday life. IoT transforms diverse applications ranging from smart homes to very critical infrastructure monitoring. The IPv6 Low Power personal area network (6LoWPAN) routes the data using the de-facto standard routing protocol for low power lossy network (RPL). The RFC 6550 of RPL protocol highlighted its insecure behavior; hence the IoT network falls prey to various attacks like version number attack, hello flood attack, increased rank, and deceased rank attack. To design an effective security solution for the mitigation of RPL attacks, a comprehensive analysis of attacks is of utmost importance. Hence this paper attempts to implement the RPL attack in the IoT network by thoroughly examining the IoT network behavior after the attacks. The paper put forth a comprehensive impact analysis of the RPL attack on the IoT network. The paper further illustrates the detailed architecture and implementation of mutual authentication. The results proved that the proposed authentication mechanism cease the entry of unauthenticated node thereby protecting the network from attacks. The proposed scheme is tested and verified with respect to power consumption and ETX metric. The results illustrate that the network not only blocks the unauthenticated node but also improves network performance.*

Keywords — *Authentication, IoT Networks, RPL Attacks, 6LoWPAN.*

I. INTRODUCTION

IoT is a novel technological paradigm that escalates conventional applications to new automation heights. IoT applications consist of the interconnection of low-power devices known as sensors, as shown in figure 1, which can automatically collect and communicate data over the internet without human intervention [1]. Various applications, including healthcare, agriculture, smart grids, environment, use these IoT-based automation techniques to enhance the efficacy of applications [2].

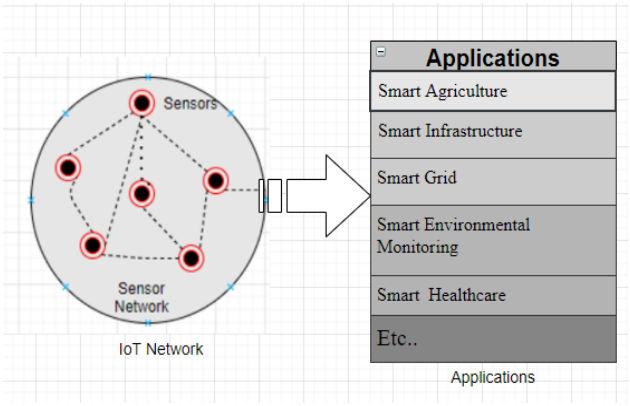


Fig 1. IoT Network and application

According to the estimation of the International Data Corporation (IDC) [3], worldwide, an estimated 55.7 billion IoT devices connected over the internet (or "things") by 2025, generating almost 80B zettabytes (ZB) of data. With such an enormous increase in IoT data, it has attracted cybercriminals to tamper with the security and privacy of the application. The IoT network consists of low-power lossy nodes deployed on a large scale. The conventional routing protocol is not appropriate for low power lossy network (LLN), the main hindrance in it is the inherent characteristics of sensor devices which include low energy consumption, low processing power, less onboard memory, low bandwidth. Therefore, the Internet Engineering Taskforce put forths the novel routing protocol for constrained device networks known as Routing Over Low Power and Lossy Networks (RPL).

RFC 6550 provides the standardization of the RPL protocol. Various applications widely use the RPL protocol as it provides an energy-efficient routing mechanism in IoT networks. However, LLN with RPL protocol is prone to various attacks because of innate properties like auto-configuration, openness, and the absence of a self-healing mechanism [4]. LLN experiences huge data loss if the attacker node manages to exploit the single sensor node. Meanwhile, the RPL protocol provides two optional security

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

modes, pre-installed security mode (PSM) and authenticated security mode (ASM). The ASM and PSM modes require the distribution and maintenance of symmetric keys, but the current RPL protocol standard does not specify this key management aspect. The key management and distribution are a strenuous task, which consumes the memory, power, and time of the network. The conventional algorithms of symmetric key distribution are not suitable for low-constrained IoT networks. This paper addresses the issue by specifying an efficient way of symmetric key distribution. Moreover, the inbuilt two security modes of RPL protocol provide the cryptographic-based defense mechanism, which requires more energy and resources [5][6]. The insecurities in RPL protocol exposed LLN to various attacks like DIS flooding attack, version number attack, increased rank attack, decreased rank attack where attacker nodes demolished the legitimate nodes. This adversely affects the performance of the network. The unauthenticated outsider or insider attacker node increases the control traffic overhead, power consumption, latency and decreases the network lifetime and reliability. Therefore, implementing the security mechanism is of utmost importance to protect the IoT network. This paper proposed the mutual authentication scheme where each sensor node authenticated itself with the root node; in turn, the root node also authenticated itself with each sensor node. The prominent advantage of the proposed mutual authentication method is i) It does not impose a computational burden and memory overhead on sensor nodes ii) Consistent performance ensures the adequate level of security iii) It is not topology dependent; the proposed model will work for any dynamic topology. The paper is structured in the following manner section 2 elaborates the RPL protocol in detail. The relevant literature survey is described in section 3. Section 4 illustrates the RPL attacks in detail. The system design and proposed methodology are described in section 5. Section 6 put forth the performance evaluation of the proposed mutual authentication scheme. Finally, section 7 concludes the paper with a future discussion.

II. RPL NETWORK INITIALIZATION

RPL is a predominant protocol for providing efficient routing with QoS support in LLN networks. The specification of RPL in RFC 6550[7] states that the RPL exhibits insecure behavior. It operates on the network layer and mainly relies on the Link layer (i.e., IEEE 802.15.4) security mechanism when operated in unsecured default mode (USM). The RPL network sensor nodes form the loop-free destination-oriented directed acyclic graph (DODAG), which is an IoT network. DODAG consists of the sink node, the source node, and the gateway node. The 6LoWPAN border router acted as a border router that routes the LLN traffic to an externally connected network, specifically termed as a cloud. A single IoT network may contain many RPL instances, and for identifying every RPL instance, the instance ID is used. The DODAG is formed using the four control messages i) DIO (DODAG Information Object) ii) DAO (Destination Advertisement Object) iii) DAO-ACK (DAO acknowledgment) iv) DIS (DODAG Information Solicitation). The initialization of DODAG is depicted in figure 2. where node 1 acted as sink node and nodes 2-9 acted as the source node. Moreover, every DODAG is identified using the unique 128-bit DODAG ID.

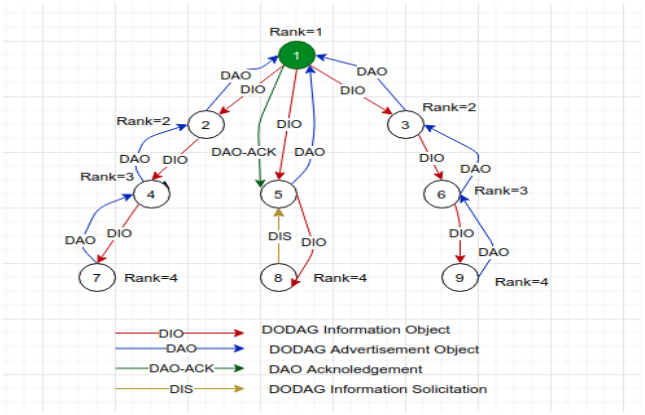


Fig.2 DODAG Initialization and Formation

Initially, the root node sends the DIO control message, as shown in figure 3 [7], which contains the control information like version number and rank of the sender message. The recipient source nodes calculate their rank using the objective function (OF) and the received version number. An OF makes use of various metrics like the Expected Number of Transmissions (ETX) or current battery power of the nodes [8]. The rank value actually depicts the node position in the network. The root node bears the lowest rank value.' G' flag of the DIO message is used for the grounded option. If not set, then the DODAG is considered floating, which means the DODAG is not connected to the remaining part of the network. If the MOP (mode of operation) is set, then it indicates the downward routing.'Prf" is a 3-bit preferable field that indicates how the root node is preferable for other source nodes in the network. Finally, DSTN is used for saving the sequence number to ensure the continuity and sequentially of the DIO message.

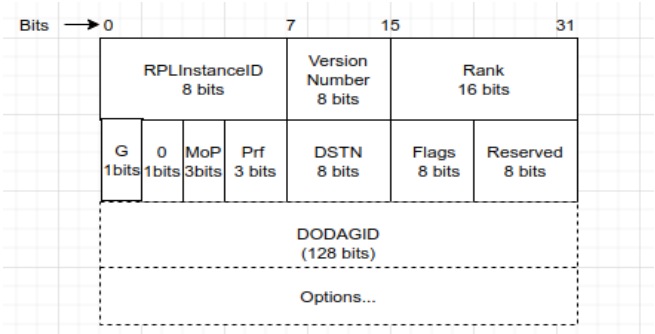


Fig.3 DIO Message Format

Once the source nodes receive the DIO message, it calculates their rank and forwards it in the form of a DAO message in the upward direction towards the root node. After

receiving all the connected node rank values, the root node gets the complete view of the network. The network connection is confirmed by the root node using the DAO-ACK message. Further, the RPL protocol uses the "Tickel Timers" to control the control traffic overhead in the network. It actually decides when the nodes should multicast the DIO message. The tickle timer interval decreases at the initial stage of the network setup and gradually increases once the network becomes stable. The attacker node resets the tickle times and increases the control traffic in the network. Resultantly the consumption of the energy in the network increases.

III. RELATED WORK

The RPL attacks proved to be dangerous for IoT networks, and many WSN researchers put forth various security solutions. However, still, the research lags in protecting the LLN from RPL specific attacks. As per the study of authors [9], among the DIS flooding, rank, local repair, and replay attacks, the DIS flooding is more adversely affects the LLN than the other attacks. The authors investigated that DIS flooding attacks adversely hamper the network configuration parameters like power consumption, delay, control traffic overhead. A similar analysis was performed by the Authors [10] for the 6LoWPAN network. The authors investigated the selective forwarding, Sybil, HELLO flooding, Sinkhole, Blackhole, Clone ID, and Local Repair attack to analyze the 6LoWPAN network throughput. The authors concluded that the entire network performance, specifically network throughput, gets adversely affected because of the increasing number of attacks. Moreover, the traditional security algorithms are not suitable for IoT networks; hence it is needed to design a lightweight defense mechanism to protect IoT networks from diverse attacks. Recently several solutions for protecting the LLN network have been proposed. In another study [11], the impact analysis of version number and DoS attack on the 6LoWPAN network is described using the Contiki-Cooja simulator, and authors highlighted that attacks increase energy consumption and reduces the battery life

The broad categories of security solutions include authentication, lightweight encryption mechanisms, Intrusion detection systems. Authors [12] understand the difficulty in RPL protocol that the protocol is not having inherent security mechanisms; hence they came up with the one-way hash chain authentication mechanism known as VeRA to detect the decreased rank attack and version number attack. In a similar line to repair the DAG inconsistency, the authors [13] proposed TRAIL mechanism, which stands for Trust Anchor Interconnection Loop used to ultimately defend against version number attack. DAG inconsistency is also protected by the dynamic thresholding method proposed by authors [14]. The identity-based signature mechanism proposed by the authors of [15] for mitigation of rank and version number attack. The authors of[16] proposed the authentication technique based on the ID provided by the server to the user and target server. This technique authenticates the user with RFID smart card and the target server. The authors make use of ECC cryptographic algorithms for the implementation of mutual authentication. The mutual authentication is performed between the target and user server. The authors of [17] proposed the authentication mechanism again based on ECC, where the sensor's private and public keys are calculated and distributed by the base station. If sensor S1 wants to communicate with sensor S2, sensor S2 will authenticate S1 using S1's public key and vice versa. In another approach by the authors [18], the authentication method was put forth to authenticate the sensor node by the neighboring sensor ID. The authors proposed the method of sending data through the authenticated aggregator node. The sink node maintains the list of authenticated neighboring nodes. Once the sink authenticates the aggregator node, the data extraction is performed.

The intrusion detection mechanism provides a strong security wall against the various attacks, and SVELTE is the most popular IDS proposed by authors [19] to detect spoofing, selective forwarding, and sinkhole attack. The machine learning-based hybrid intrusion detection system is proposed by the authors [20] using the map-reduce approach. Certainly, the machine learning (ML) based IDS consumes more energy. Hence they are unsuitable for IoT networks. Also, ML, the major problem in the low constrained network, is the collection and labeling of data. Moreover, ML-based IDS efficiency is not yet realized on real 6LoWPAN networks.

Authors [21] argued that despite two inherent RPL security mechanisms mentioned earlier in section 1, ASM and PSM, it does not define the implementation way-out and key management procedure. Moreover, most 6LoWPAN-RPL security solutions are not efficient and suitable for protecting the IoT system against various attacks. This literature survey also ratifies the same; hence this work proposed the lightweight mutual authentication technique to mitigate the RPL specific attacks.

IV. RPL ATTACKS

The RPL standardization RFC 6550[7] highlighted the insured behavior of the RPL protocol. The 6LoWPAN with RPL protocol is exposed to various attacks, which are broadly categorized into three types. i)The attacks consume the LLL's power, memory and energy by exhausting the resources. These types of attacks drain the resource-constrained devices and demolish the network's node completely. ii)The attacks mainly target the topology of the network; these attacks try to disturb the topology and isolate one or more nodes from the network. iii) The attack of this category sniffs the traffic, performs reconnaissance to explore the vulnerabilities of the network. As per the literature survey, the imperative RPL attacks are discussed below.

A. HELLO flood attack

In RPL, a Hello flood attack is caused due to the multicasting or unicasting of DIS messages by an attacker node. DIS is the solicitation messages sent by the new node for joining the IoT network. The new node, after a fixed interval, transmits the DIS messages to get the DIO messages from the neighboring nodes. However, the time interval for sending the DIS message is not specified in RFC 6650 [7].Upon receipt of the DIS message, receiver nodes multicast the DAO messages after resetting their tickle timer. After the new node receives the DIO message from any of its neighboring nodes, it stops sending the DIS messages, sends an acknowledgment in the form of a DAO message, and joins the network. The attacker takes undue advantage of this fact and chooses the very small DIS transmission interval to flood the network. This is known as the hello flood attack, as shown in figure 4.

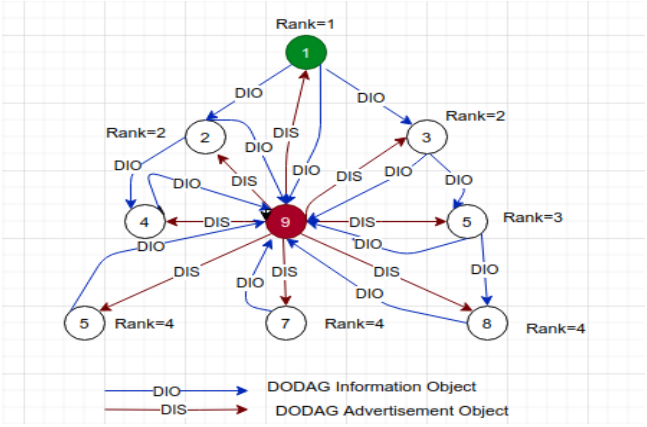


Fig.4 Hello Flood Attack

The neighboring node, upon receipt of the DIS message from an attacker node, force to broadcast the DIO messages, which further increases the control message traffic, thereby increasing the power consumption and decreasing the network lifetime.

HELLO, flood attack is demonstrated in figure 4, where the node ID -1 acted as sink node and node ID 2to 8 acted as the source node. The node with ID-9 acted as an attacker node, which floods the network with the numerous DIS request message. As per the specifications of RPL protocol the network flood with the DIO messages. The control traffic overhead of the network increases tremendously and certainly the battery life of the nodes decreases which may lead network to halt.

B. Version Number Attack

The RPL version number attack is caused due to illegitimately incrementation of the version number by the attacker node. An attacker node transmits the DIS message intending to get the DIO message from the neighboring node. In this attack, the attacker node unicasts the DIS message after the fixed interval until it receives the DIO message. Upon receipt of the DIO message, the attacker node modifies the version number field and forwards it to the neighboring nodes. RFC 6550 [7] does not specify any authentication mechanism for verification of the version number in the received DIO message. Hence upon receipt of the DIO message with the changed version number, they consider that their routing table entries are outdated.

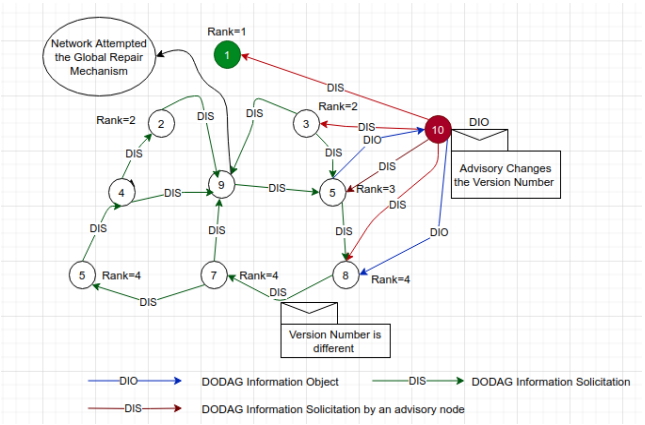


Fig.5 Version Number Attack

This illegitimate version number value is circulated in the entire network using the DIS message resultantly, the entire network experiences loop and attempted the global repair mechanism. This mechanism is used to repair the network from loops, but this mechanism drains the resources, power, memory, and lifetime of the network. The attacker node slowly destroys the network by repeatedly changing the version number. The detection of a version number attack is a difficult task as the change in routing parameters and energy consumption is very less. Figure 5 illustrates the version number attack where node 10 acted as an attacker node and node 1 to node 9 are genuine nodes. In the first step, an attacker node broadcasts the DIS message in return in the second step it receives the DIO message from the genuine node. Advisory changes the version number and forwards the DIO to the neighboring node. The genuine node accepts the change in version number and make their routing entries obsolete. The change in version number is circulated in the network using the DIS message, hence the nodes calculates their new rank and entire network attempted the global repair mechanism.

C. Rank Attack

The rank property of the RPL protocol` plays a very important role in the uninterrupted operation of the protocol. The main properties of the rank are i) The rank values given the information about the position of the node in the network. ii) The rank value is used to choose the preferred parent iii) The rank prevents the formation of loops and maintains the control traffic overhead. The drawback of the RPL protocol is that no authentication mechanism is provided for the validity of the received rank value. The advisory node changes the rank values to disturbs the network's traffic

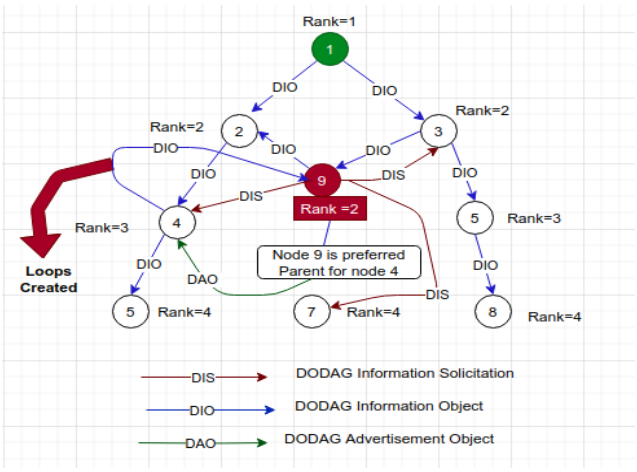


Fig.6 Rank Attack

. The advisory performs the rank attack in any of the following three ways,

i)The advisory node 10 as sown in fig 6 chooses and sets its rank values equal to the rank value of any neighbor. Resultantly the network experiences loops which certainly increases the network traffic and makes the network unstable.

ii)Secondly, the advisory node advertises the higher rank values using the DAO message to its neighbor. Hence the entire parent-child relationship in the network changes and networks experience loops. This attack is known as an increased rank attack.

iii)At last the advisory node advertises the lower rank value and hence it becomes the parent for descendant nodes. Resultantly, the genuine node chooses the advisory as the preferred parent and routes all its data towards the advisory node. This attack is known as a decreased rank attack.

Rank attacks increase the control traffic overhead hence expected transmission count (ETX) also increases, beacon interval decreases which ultimately increases the power consumption of the network.

V. PROPOSED SOLUTION

Proliferation of unauthorized node in the IoT network severely affects the network performance. The proposed mutual authentication scheme ceases the entry of unauthorized node by providing the two-way authentication for sink and source nodes. The efficient key distribution and management approach proposed by the authentication scheme is best suitable for LLN's network as it consumes the less computing resources, memory and power. The notations used by the proposed mutual authentication scheme is stated below in table 1.

The scheme begins with the consideration of the one RPLInstance in DODAG with one sink node and the remaining source nodes. The system design of the proposed scheme is shown below in Fig.7.

Table 1. Notations parameters used in proposed method.

Parameters Used	Description
RI_{Sink}	Initial Random Number generated by Sink node
RI_{Source}	Initial Random Number generated by the source node
K_a	The symmetric key shared between the source and the sink node
$E(RI_{Source})$	The encrypted random number at the sink node
$E(RI_{Sink})$	The encrypted random number at the source node
RA_{source}	Authentication code generated at the sink node
RA_{sink}	Authentication code generated at the source node.
RRI_{sink}	Regenerated RI_{Sink}
RRI_{source}	Regenerated RI_{Source}

In the 1st step, at the time of network initialization, the sink node generates the initial 8-bit random number RI_{Sink}. The sink node stores the value in its memory and then transmits $RI_{Sink}$to the source node. Upon receipt of this RI_{Sink} the source node sets the flag value in the DAO control message [7] as 1, which not only indicates the starting of a new session but also ensures its genuinity too.

In the 2nd step, the source node generates another random number of 5 bits. Source node upon storing the random number in its memory transmits it towards the sink node using the flags bit of DIS control message [7]. As per RFC 6550, flag bits are not used in the communication. The random number generated by the source node is termed asRI_{Source} which is transmitted to the sink node using the DIS control message.

In the 3rd step, at the sink node, the received 5-bit value of $RI_{Source}$is padded to the length of authentication key K_a. The key K_a is the same as the 8-bit value RPLInstanceID.The RPLInstanceID is the field in each control message used to identify the unique RPLInstance of DODAG. This value cross-checks whether the node belongs same RPL instance of DODAG. This research uses this unique 8bits RPLInstance ID as the value of the key for authentication purposes. Further sink node performs the $cross\ (RIsource \oplus Ka)$ and Rotation operation as given below.

$Cross\ (RIsource \oplus Ka)$

The cross operation at first pad 5-bit RI_{Source} value to the length of the 8-bit key. The RI_{Source} is padded by three 0 bits to make $RIsource = \text{Ka}$ The cross operation further performs the XOR between $RI_{Source}$and K_a to generate the encrypted value of RI_{Source}.as shown in equation number 1.

$$E(RIsource.) = RIsource \oplus Ka \quad (1)$$

Rotation E(RIsource)

The Rotation is performed on E($RI_{Source.}$) which include the circular left shift of E($RI_{Source.}$) by 1 bit to generate the value of authentication code AC_{source}givenbelow by equation number 2

$$ACsource = (E(RIsource)) << 1 \quad (2)$$

Further, the authentication code (AC_{source}) is transmitted from sink node to the source node.

In the 4th step, at the source node, similar operations are performed as given below in equation number 3 and 4, firstly the $cross(RIsink \oplus Ka)$operation is performed on the received value of RI_{Sink} to get the encrypted E($RI_{Sink.}$).

$$E(RIsink.) = RIsink \oplus Ka \quad (3)$$

The E($RI_{Sink.}$) is further circularly left shifted by 1 bit to get the authentication code for Sink node AC_{Sink}, which in turn is transmitted towards the sink node.

$$ACsink = \big(E(RIsink)\big) << 1 \quad (4)$$

The 5 th step is executed at the source and sink node simultaneously. The exact reverse mechanism was executed on AC_{sink} and AC_{source} at sink and source nodes respectively to get the values of RI_{sink} and RI_{source} back. To give a clear understanding, these values are renamed as regenerated RI_{sink} (RRI_{sink}) and regenerated RI_{source} (RRI_{source})

Further, in the 6th step, the sink node compares the initially generated RI_{sink} with RRI_{sink} and the source node compares RI_{source} with RRI_{source}, if the values are equal then the sink and source node agree with the authentication mechanism and the proposed mutual authentication protocol completed.

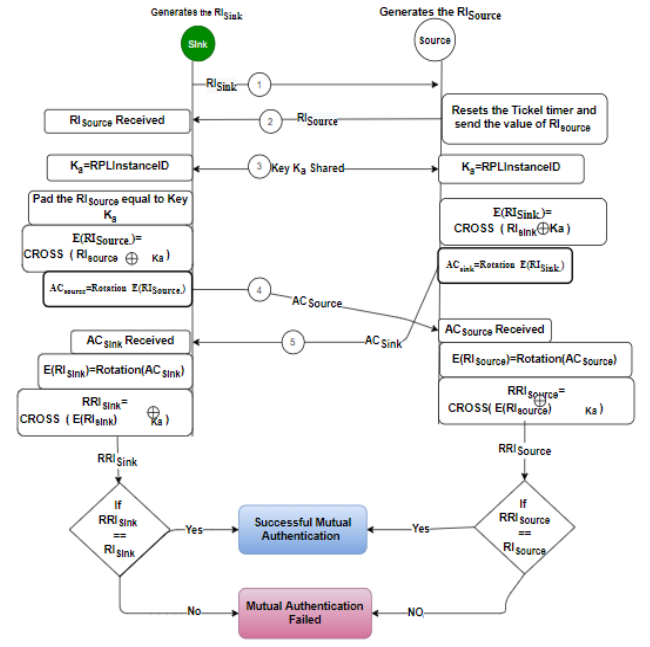


Fig.7 Proposed Mutual Authentication

VI. PERFORMANCE EVALUATION

In thissection, the experimental setup for validation of mutual authentication is discussed. The mutual authentication is evaluated on the basis of power consumption and control packet overhead.

A. Experimental setup

To study the impact of RPL attacks on 6LoWPAN network and also to evaluate the performance of the proposed mutual authentication scheme, the Contiki 2.7 operating system is for experimentation. Contiki is the popular lightweight operating system for IoT networks. It provides eminent support for all the protocols of the IoT protocol stack which include IEEE 802.15.4 (Physical and MAC layer),6LoWPAN (adaptation layer), RPL (network layer), UDP (transport layer)CoAP(Application Layer). Contiki includes all the fundamental mechanisms of RPL protocol. It provides its compatibility with the various hardware platforms. The cross-level network simulator is provided by the Contiki operating system termed as Cooja. Hence this paper uses the Contiki-Cooja which provides the real results. The Cooja simulator consists of various sensor nodes termed motes, this paper uses the T-mote sky for experimentation. The hardware specification of T mote sky is given in table 2. Further, table 3 displays all the Cooja simulation parameters used for experimentation. The RPL attacks are launched by manipulating the ContikiRPL library, the network contains the one malicious node.The node is positioned close by the root node to examin the utmost impact of control messages on the network. The network shown in fig 9 is termed a reference network which is used for performing the experimentation. The network consists of one sink node with node ID 0 and 21 source nodes. Later the attacks hello flood, version number, and the rank attack launched one after the other using the attacker node with the highest ID (ID-22), the network shown in fig 10 depicts the attacker node position. This paper analyzes the comparative impact of the hello flood, version number, and rank attack on the RPL network. The experimentation further illustrates the mitigation of attacks using the execution of the proposed security scheme of mutual authentication.

Table 2. Hardware Specification of Tmote Sky

Parameter	**Range of Values (Normal-Maximum)**
Supply voltage	2.1-3.6v
Current Consumption: MCU on, Radio RX	21.8 -23 mA
Current Consumption: MCU on, Radio TX	19.5- 21 mA
Current Consumption: MCU on, Radio off	1800 -2400 µA

Current Consumption: MCU idle, Radio off	54.5 -1200 µA
Current Consumption: MCU standby	5.1 -21.0 µA
RAM,, and 128B of information storage	10kB
flash	48kB

Table 3. Simulation Parameter

Simulation Parameter	Values
Simulation tool	Contiki 2.7 Cooja simulator
Mote Type	Tmote Sky
Network layer Protocol	RPL
PHY/MAC layer Protocol	802.11.15.4
Total number of maliciousnodes	1
Radio Medium	UGDM:(Unit Disk Graph Medium) Distance Loss.
Transmission range	50m
Interference Range	100m
Mote Start Delay	100ms
Positioning	Random Positioning

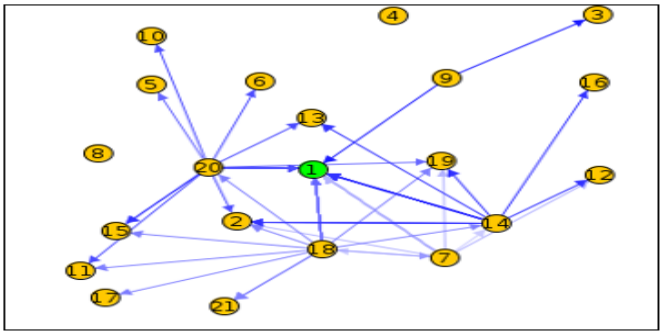


Fig.9 Reference Network

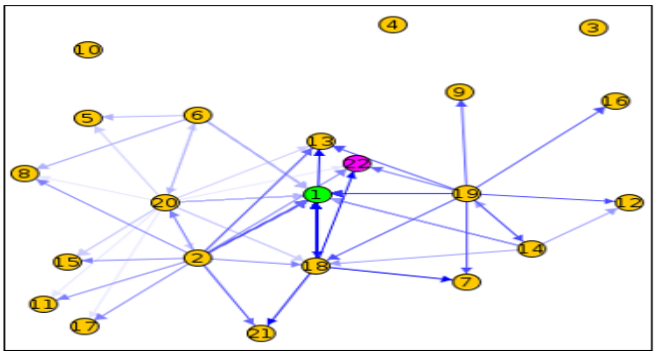


Fig.10 Attacked network

B. Performance Metrics

The performance evaluation of the proposed mutual authentication scheme is based on the following metrics.

***i)Power Consumption*: -**The total power consumed is measured as a combination of CPU power, LPM power, transmit power, and received power. The LPM is the low power mode of the sensor device which indicates the power consumed by the node during sleep mode. The transmit and received power indicates the power required for transmitting and receiving the control traffic.

***ii)ETX*-**It is the expected transmission count which determines the reliability of the network. ETX specifies the value of the number of transmissions done for a successful delivery of the message from source to destination. Reliability and ETX are inversely proportional, the lower the ETX the better the reliability.

a) Power consumption: This section discusses the impact of RPL attacks on the power consumption of IoT networks. In this respect, this paper thoroughly analyzed the CPU and LPM power consumed by the nodes. The figure 11 shows the CPU, LPM power consumed by the network node under RPL attacks. The power consumption clearly indicates that the attacked network nodes consumed more power thereby depleting their battery life. The experimentation results indicate that the hello flood attack causes severe damage to the network node as compared to other RPL attacks. The figure 11 depicts the power consumption of the proposed mutual authentication technique, the authentication mechanism prevents the node from getting connected with the network nodes as the authentication of the attacker node fails as shown in fig.11

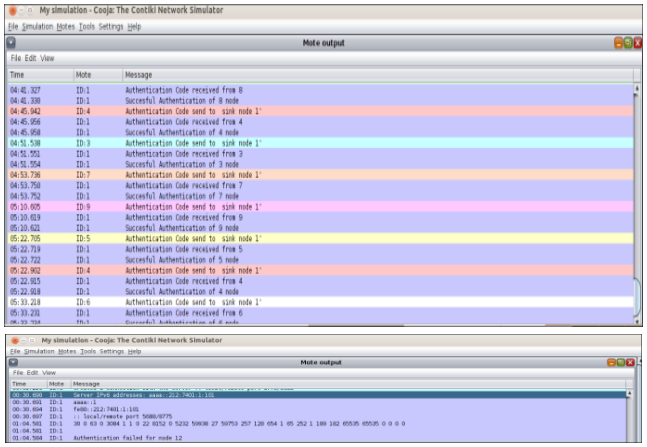
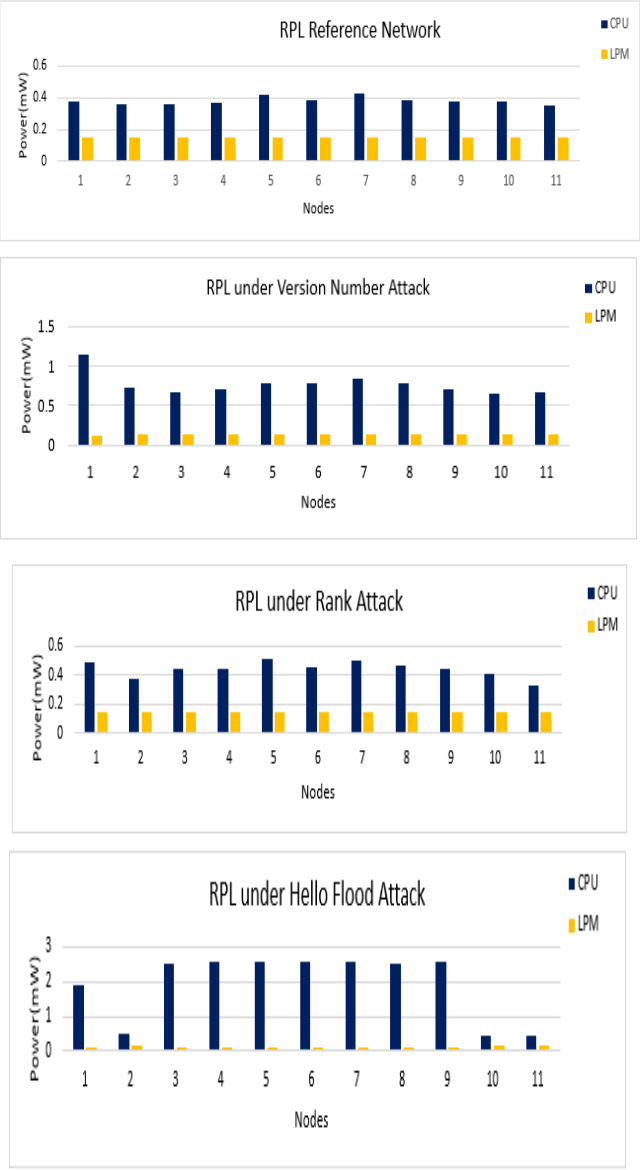


Fig 11 Screenshot of mote output of proposed method

The CPU consumption of network nodes with the proposed authentication mechanism is less than the network under attack because the node simply discards the attacker node's malicious DIS messages thereby preventing the unnecessary reset of the tickle timer. The LPM consumption of the nodes increases as network nodes attempt the sleep mode for discarding the malicious packets. The nodes save their battery life by attempting the LPM modes thereby increasing the network lifetime. As discussed in the section 3 the attacker node position in the network causes an impact on the nodes, the nodes 5,6,7,8 are close to an attacker node,

hence their power consumption increases. Whereas nodes 11,2,10 reside away from an attacker node hence their power consumption is lower. The figure 12illustrates the hello flood attack, version number attack and rank attack CPU and LPM consumption. The hello flood attack damages the network severely and the highest CPU power consumption of node 5 (≈2.587mW) and the LPM of the reference node 5 is (≈0.085mW). We have kept the same topology as indicated in fig 8 to observe the CPU power consumption of node 5 after implementation of the proposed authentication algorithm in the attacked network, which is (≈0.354mW) and the LPM power consumption of the same node is (≈0.153mW), hence it is proved that the proposed authentication mechanism restricts the attacker node from damaging the network.



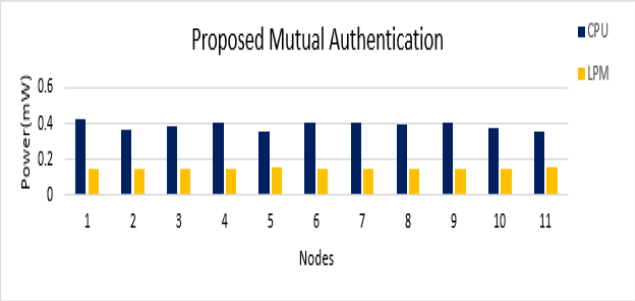


Fig 12. CPU and LPM power consumption by every node of Reference and Attacked network

b) ETX: Expected Transmission Count is the number of transmissions required by the node for successfully delivering the message to the destination node. In RPL, the minimum rank with hysteresis objective function (MRHOF) metric uses ETX for calculating the least-cost distance between any two nodes. The "RPL Probing" mechanism of Contiki is used for testing the quality of the link. The ETX value is updated after transferring the encapsulated ICMPv6 control messages (DIO, DIS, DAO, DAO-ACK) to the preferred parent node. Hence the greater the value of ETX lower the quality of the link. The RPL attacks disturb the routing resulting in an increase in ETX value. The experimentation results depicted in fig 13 indicates that the version number and rank attack disturb the entire routing and forces the network to attempt a global repair mechanism. Hence the ETX value is greater in version number attack and rank attack as compared to hello flood. Whereas, in hello flood attack the nodes are busy in receiving they can hardly transfer the data, hence the calculated ETX count is lower than version number attack.

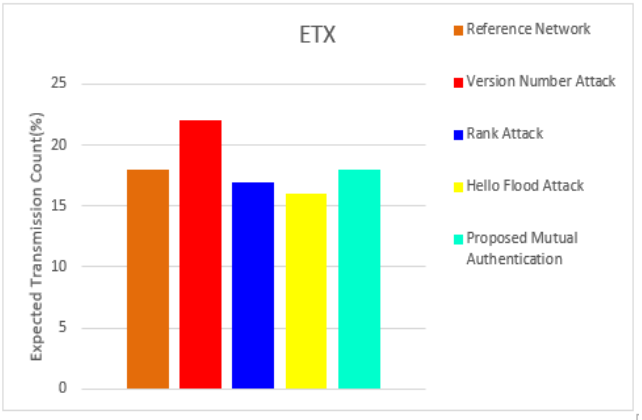


Fig13: ETX consumption of proposed method.

The proposed authentication method is tested for all the RPL attacks mentioned above, and the average ETX value was observed. The proposed method forbids the attacker node entry in the network, thereby keeping the ETX count approximately the same as of the reference network. Thus, the proposed authentication scheme is appropriate for protecting low power lossy 6LoWPAN network.

VI. CONCLUSION

Escalation in the IoT technology benefited the various applications. The efficiency and performance of the applications highly increase which provides excellent services to end-users. However, protecting such resource-constrained IoT-based applications from various threats and attacks is the biggest challenge. This research proposed the mutual authentication mechanism, which requires some changes in the existing standard of RPL protocol to provides a robust defense against the various RPL attacks. The paper put forth the detailed result analysis of the authentication mechanism against the version number, rank, and hello flood attacks. The simulation results prove that the proposed authentication mechanism forbids the unauthenticated node to enter the network and protects the network. The paper examined the comparative results of the reference network built using the existing RPL protocol and the proposed authentication mechanism. Mutual authentication imposed very less overhead on the RPL network but in turn, it provides adequate security to low constraint IoT network.

REFERENCES

[1] Da Xu L, He W, Li S. Internet of Things in industries: a survey. IEEE Trans Ind Inform, 10(4) (2014) 2233-2243

[2] Mihovska A, Sarkar M. Smart connectivity for the Internet of Things (IoT) applications. In: New Advances in the Internet of Things. Cham, Switzerland: Springer; (2018) 105-118.

[3] IDC. The growth in connected IoT devices is expected to generate 79.4ZB of data in 2025, according to a new IDC forecast. 2019. Accessed September 21 (2019).

[4] Musaddiq A, Zikria YB, Hahm O, Yu H, Bashir AK, Kim SW. A survey on resource management in IoT operating systems. IEEE Access. 6(2018) 8459-8482.

[5] Ghaleb B, Al-Dubai AY, Ekonomou E, et al. A survey of limitations and enhancements of the IPv6 routing protocol for low-power and lossy networks: a focus on core operations. IEEE CommunSurv Tutor., 21(2) (2018) 1607-1635.

[6] Malik M, Dutta M, Granjal J. A survey of key bootstrapping protocols based on public key cryptography in the Internet of Things. IEEE Access. 7(2019) 27443-27464.

[7] Vasseur, J., Agarwal, N., Hui, J., Shelby, Z., Bertrand, P., &Chauvenet, C. RPL: The IP routing protocol designed for low power and lossy networks. Internet Protocol for Smart Objects (IPSO) Alliance, 36(2011) .

[8] Brachman, A. (2013). RPL objective function impact on LLNs topology and performance. In Internet of things, smart spaces, and next generation networking, (2013) 340-351. Springer, Berlin, Heidelberg.

[9] Le A, Loo J, Luo Y, Lasebae A. The impacts of internal threats towards routing protocol for low power and lossy network performance. In: Proceedings of the IEEE Symposium on Computers and Communications (ISCC); (2013) Split, Croatia.

[10] Abhishek Verma and VirenderRanga "Analysis of Routing Attacks on RPL based 6LoWPAN, International Journal of Grid and Distributed Computing 11(8) (2018) 43-56 http://dx.doi.org/10.14257/ijgdc.2018.11.8.05

[11] Smita S. Ambarkar, N.M.Shekokar Critical and Comparative Analysis of DoS and Version Number Attack in Healthcare IoT System ,Proceeding of First Doctoral Symposium on Natural Computing Research, DSNCR (2020).

[12] Dvir, A.; Holczer, T.; Buttyan, L. VeRA—Version Number and Rank Authentication in RPL. In Proceedings of the 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems, Valencia, Spain, (2011) 709–714.

[13] Perrey, H.; Landsmann, M.; Ugus, O.; Wählisch, M.; Schmidt, T.C. TRAIL: Topology Authentication in RPL. In EWSN '16 Proceedings of the 2016 International Conference on Embedded Wireless Systems and Networks; Springer: Berlin/Heidelberg, Germany, (2016) 59–64

[14] Mayzaud A, Sehgal A, Badonnel R, Chrisment I, Schönwälder J. Mitigation of topological inconsistency attacks in RPL-based low-power lossy networks. Int J NetwManag. 25(5) (2015) 320-339.

[15] Aris, A.; ÖrsYalçın, S.B.; Oktug, S. New lightweight mitigation techniques for RPL version number attacks. Ad Hoc Netw., 85(2019) 81–91. https://doi.org/10.1016/j.adhoc.2018.10.022.

[16] J. H. Yang and P. Y. Lin, An ID-based user authentication scheme for cloud computing, in 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, (2014) 98–101.

[17] F. Chu, R. Zhang, R. Ni, and W. Dai, An improved identity authentication scheme for internet of things in heterogeneous networking environments, in 2013 16th International Conference on Network-Based Information Systems, (2013) 589–593.

[18] S. Peng, An Id-based Multiple Authentication scheme against attacks in wireless sensor networks, in 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems, 3(2012) 1042–1045.

[19] Raza S, Wallgren L, Voigt T. SVELTE: real-time intrusion detection in the Internet of Things. Ad Hoc Netw. 11(8) (2013) 2661-2674

[20] Bostani H, Sheikhan M. Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on MapReduce approach. Computer Communications. 98 (2017) 52-71.

[21] Y. Tian, G. Chen, J. Li, A new ultralightweight RFID authentication protocol with permutation, IEEE Communications Letters, 16(5) (2012) 702-705.