iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** V **Month of publication:** May 2018

DOI: http://doi.org/10.22214/ijraset.2018.5406

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

A Study of Routing Protocol and Security Scheme for Cloud-Connected Smart Home Internet of Things Devices

Divya V[1] Kiran V K[2]
[1]*PG Scholar,Computer Science and Engineering NSS College of Engineering* Palakkad,Kerala,India
[2]*Assistant Professor, Computer Science and Engineering NSS College of Engineering* Palakkad,Kerala,India

***Abstract**: With IoT many applications and services have been emerging in the areas such as, smartcities, surveillance, healthcare, security, etc. The services offered can be ubiquitously accessed through smart device applications by the users. The interaction between smart devices and cloud based web services is a common scenario of IoT deployment. Security is a major concern in IoT and some papers have proposed a secure communication channel between the users and devices of a smart home in terms of authentication, authorization and antitheft mechanism. However, a reliable communication is considered in most of the cases. In this paper,a study is conducted by assuming a lossy communication channel and thus the employment of a suitable routing protocol to an existing IoT security system.*
***Keywords**: IoT, Smart-home, Authentication, Authorization, Antitheft, Lossy Communication*

I. INTRODUCTION

The Internet of Things (IoT) is an important factor in many areas of our society. IoT brings intelligence to critical aspects like transportation, industry, payments, health and so on.IoT comes with a promise of smart world where intelligent devices form collaboration with each other to exchange information among them as well as gather information from the environment and take appropriate decision. IoT applications have come a long way from being inflexible industrial things to market- available products that can cater to the needs of common people.

IoT devices are collecting data from individuals and sharing with third parties such as voice recognition or figure print while playing video game or accessing different devices. Attacker can use these kinds of data which can pose a privacy problem for those who are unaware of the presence of the devices and have no meaningful influence over how that collected information is used. IoT is still new technology which still needs to develop application standard, communication protocol as well as secure centralized data service which can be used worldwide. IoTs strict security policies are though creating a wall which blocks its vast adoption. [2].

The adoption rate of these computing elements, especially in the smart home area, depends on the security level provided by the applications. Privacy is an important element for regular users and the IoT (Internet of Things) enabled application application deployed in a smart home must be designed with a robust security mechanism [3]. The implementation of security and privacy features raises a functionality issue, because an IoT solution comprises multiple elements: embedded devices, user interface elements, cloud computing for data processing,device control etc .

Another thing to be of concern is that the communication over this type of network channels cannot be reliable as it is of no certainty that the correctly intended object received a message sent by another object. There is a chance that the message could be disrupted partially or even fully because of any physical hindrance or some other noise source. This not so reliable nature of the communications in embedded object networks is called as being 'lossy'. Such networks are also referred to as Low power and Lossy Networks (LLNs). In a lossy communication channel retransmitting the security messages will lead to some delays and the presented security protocols will have to be redesigned in order be packet loss tolerant.

The process by which the network determines what path(s) the messages should take through the network is known as routing. Routing in LLN should keep an eye on the above issues and treat this as input requirements for design. The routing protocol design in this type of network must take care of how much data a network can hold,process etc.Also it should track the devices' capabilities, speed etc.

In coventional networks any loss of connectivity will lead to the quick re-convergence and finding of alternate routing paths. This is required so that data traffic is re-routed as soon as possible if there are any network failures and with as little loss of data. For that,

many techniques such as Fast Reroute for IP/MPLS have been designed for link state protocols such as OSPF,ISIS and so on.A preferred model in this case should be able to 'under-react' to the transient connection loss and have a confidence-monitoring model before triggering a full reconvergence. Furthermore, routing in LLNs should be able to self manage to a great extent and be able to heal itself without requiring manual intervention.

IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) has come as a main solution to address this topic.[14] RPL is designed to run on routers with limited processing power, memory, energy supply etc. It deals with links that can have time-varying quality and high loss rates. Furthermore, RPL targets to support large networks that can scale to thousands of nodes.Some of the fetures of RPL are : Its support of dynamic routing metrics and constraints,storing and non-storing
nodes,loop avoidance and loop detection,global and local repair,timer management etc. In this paper, RPL has been employed to this smart home network.

II. RELATED WORK

Mobile as well as embedded devices need better authentication techniques in order to be deployed in security sensitive areas. Multiple authentication techniques have been developed and employed today.But in case resource constrained devices, there are not many standardized solutions accepted by software developers and hardware manufacturers available. In [4] Lindemann et al. present a universal authentication framework protocol which enabled a passwordless authentication mechanism which got its name like 'FIDO'. This protocol is adopted by many organizations and has a great market value. This FIDO protocol is used as a first factor authentication mechanism and makes use of cryptographic keys in place of passwords. The FIDO cryptographic keys are stored in a module called authenticator which is unlocked by the user using biometrics or other security mechanisms.

Even though FIDO was designed to address security issues on smart phones, the protocol is acceped in the areas of IoT devices as well. For example, Hannes Tschofenig argues in [5] that an FIDO architecture can be applied to an IoT network. In this paper,the most important IoT design patterns were deployed: the cloud based and local area based connectivity. The author presents a security architecture where users can authenticate to the IoT device by using a federated protocol. The last scheme uses OAuth along with the FIDO protocol. This work also stresses the importance of the security by design principle when developing an IoT software product.

An effort to contribute like FIDO was done by Frank Stajano in designing PICO [7],which also is a security system focussing on the authentication problem.PICO also employs cryptographic keys for a passwordless authentication mechanism, the system being scalable and feasible for embedded devices. Moreover PICO gives an ample solution for making the devices theft-resistant and loss resistant.This is enabled by implementing a keep-alive protocol between the IoT devices owned by the same user. Securing the communication between the IoT devices is a critical issue from the security point of view. A lot of work has been done in this direction, with DTLS as de facto standard. In the IoT paradigm,DTLS is used in conjunction with CoAP (Constrained Application Protocol). Beside using digital certificates, a DTLS session can authenticated using pre-shared key mechanisms or raw public keys. are not standardized they often follow the same design pattern having similar security requirements.

In [10] Raham et al. show a general scheme where IoT devices are integrated with a cloud environment. The latter presents the vulnerabilities and the security issues which must be handled by the IoT systems. It presents an authentication and authorization framework for the IoT cloud connected devices. The scenario presented in the previous work consists in an embedded network where the data between the sensor and the actuator is transfered using a cloud system.In a smart-home environment the devices provide complex services by interacting with each other, thus communicating with a trusted and uncompromised module is critical.

One authentication method used for constrained devices is the use of users biometric such as finger print [15]. This method, when applied for WSN, requires the users to register their biometrics with the base station before they can access the data. It requires the following four steps to complete the authentication process: rstly, in pre-deployment phase the base station assigns a unique ID and generates a unique master key for each sensor in the network. Secondly, in the registration phase, the user registers his biometric and offers his/her identity and password to the base station in a secure manner. Then, based on a hashing method applied on the biometric, the base station generates a master card and securely sends it to the user. The third phase is the login phase in which the user enters his smart card and his biometric information to a terminal device. If biometric information is veried successfully, the user enters his password to allow the smart card to verify his identity and password. Finally, the base station authenticates the user base on a series of hashing values.

In [1], a lightweight security stack has been presented where users can authenticate to their smart home IoT devices through an untrusted cloud system.A passwordless authentication method using FIDO is proposed, where the FIDO server is a module hosted by the IoT device, deployed in a smart home scenario. The proposed solution is a practical one and it is tested using one of the most

mature cloud software stack for IoT devices.The FIDO security solutions is augmented with PICO elements in order to provide a theft-resistant solution and added to FIDO a privacy preserving extension in order to protect the user identity and to permit an attribute access controlled method to the IoT device for administrative purposes.The security solution proposed in this work can be integrated in an already existing software and hardware architecture, requiring minimum costs from the user side. Among other things, this work encompasses security elements described in the related work papers and proposes a complete architecture with a clear vision regarding the software product life-cycle.

III.SYSTEM ARCHITECTURE

The system architecture consists of four main entities: the smart home IoT devices, the cloud platform , a smart-phone management application and a routing protocol. The first module consists of different IoT devices deployed in a smart home environment.The second module is the cloud platform which process the IoT devices data.In this scenario the cloud platform is treated like an untrusted module, though it can be not malicious too. The cloud platform may be administered by a device maker or can be a third-party service. This system has two main tasks: processing and transport of the data. The data processing service can be aggregation of data, machine learning services etc. The second tasks enables the communication between the user and the devices or between the different devices of different locations.The third module is the smart-phone management application which is used to control the smart home devices remotely.And the last module,RPL is a Distance Vector IPv6 routing protocol for Low Power and Lossy Networks (LLNs) that specifies how to build a Destination Oriented Directed Acyclic Graph (DODAG) using an objective function and a set of metrics/constraints.

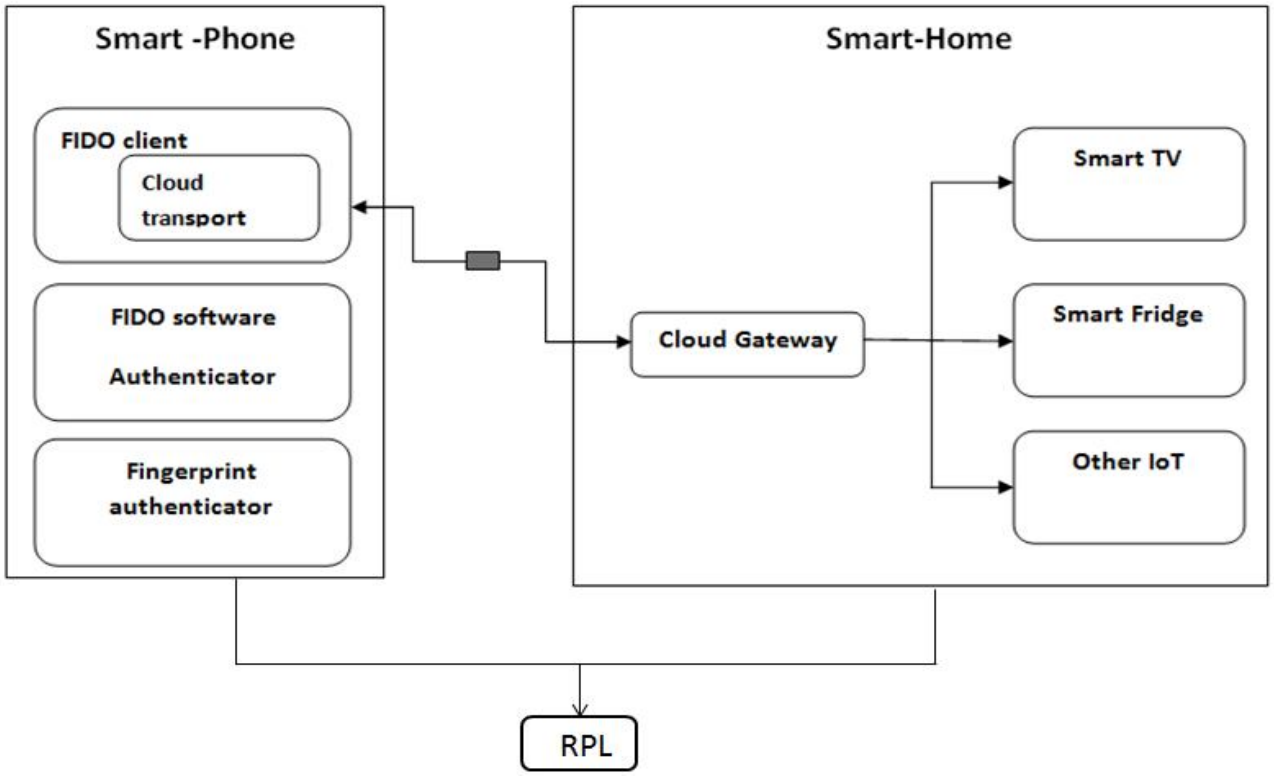


Fig 1: General Security Scheme

The security system general scheme is presented in Figure 1. For the authentication mechanism, the FIDO UAF (Universal Authentication Framework) protocol was chosen. FIDO UAF is a passwordless first factor authentication protocol developed by the FIDO Alliance. This protocol has cryptographic key pairs stored in an 'authenticator' module. In order for the keys to be used, the user will have to unlock the authenticator using biometrics, pin or other security techniques. The reason for choosing FIDO is that it is greatly supported by smart phone companies.The IoT device is the FIDO server and an Android management application controlled by the user, behaves like the FIDO client. The authenticator module has a software implementation which is enabled by having OpenTEE in order to have a Trusted Platform Module Interface.

The working of the system is as follows.If a user buys a new IoT device, it must be installed in the smarthome environment. The device install has some steps. The first step is a user-to-device registration procedure.This procedure in volves the imprinting of embedded device with the user FIDO public key. This process can take place only if the device is not imprinted with some cryptographic key already.For the registration to start, the user should give a proof to the IoT device in form of a proper authorization. This feature is materialized by adding a FIDO extension that comprises of an authorization data, calculated using a privacy preserving attribute protocol. In this case, the device manufacturer gives a an anonymous token to a user who purchased the device. The user gives this token in a customized FIDO registration protocol. By running this protocol, the IoT device knows that the user who wants to imprint its FIDO public key is a real buyer from the device manufacturer.

By employing this security scheme, the device cannot find any information which affects the user privacy because a creation of an account is not done. This can be simply elaborated by the device maker by making use of multiple attributes, in connection with the smart object purchased by the user. At the time of registration, the IoT device must display to the FIDO client ,which is mostly an Android management application a list of approved authenticators. Like this, the IoT device can choose only the FIDO authenticators that are trusted. This is a characteristic of the FIDO protocol. While engaging in the registration procedure, the client side authenticator should sign a random challenge made by the device using an attestation key.An X.509 attestation certificate is kept along with the associated private key by the authenticator. This attestation certificate will have been signed by the authenticator module producer. The attestation method gives permission to the IoT device to trust another authenticators which are third parties with the aid of trusted attestation certificate system.

An environment where the smart home IoT devices and cloud platform are connected needs a peculiar data flow between the evices and the cloud. The cloud platform can make queries to the IoT devices for extracting certain data particular for some applications. Also,this could lead to the issuance of certain commands by the cloud platform aimed to the device. These commands could break with a user defined policy, which may lead to a breach of security. This paper studies about an authorization framework by FIDO, where every command by the cloud to the IoT device must go through an authoriation process by the user. When the cloud tries to query or process some device data, the user does an calculation of an authorization policy which must get an user approval. And the user gets the authorization policy by the help of a protocol extension of FIDO.

In the first step there comes a request from the cloud module to the IoT device. In case the IoT device detects the request as unauthorized, it directs the cloud platform straight to the user's device,say smart phone. Then the authorization policy is displayed to the user in a suitable user interface. If the user approves of the data requested by the cloud platform it starts a FIDO authentication protocol with the smart device. After the FIDO authentication occurs, the cloud platform is signaled by the user to request the data again. During this time the IoT device does a comparison of the policy data by checking in a local policy database. Only If the hash of the policy is authorized, the requested data gets delivered to the IoT device. By using such a policy, the communication occurring between cloud and a smart device or the communication between different devices can be controlled and authorized by the user.

Since all these communications cannot be considered as reliable,a routing protocol is employed. RPL: an open routing protocol for IP smart object networks standardized by the IETF is used here. RPL(Routing Protocol for Low power and Lossy networks) is a Distance Vector IPv6 routing protocol for LLNs(Low power and Lossy networks) that specifies how to build a Destination Oriented Directed Acyclic Graph (DODAG) using an objective function and a set of metrics/constraints. The objective function operates on a combination of metrics and constraints to compute the 'best' path. Each deployment comes with different objectives.So there can be several objective functions in operation on the same node and mesh network. Also a single mesh network may need to carry traffic with various requirements of path quality. For example, several DODAGs may be used with the objective to find paths with best Expected Transmissions values and avoid non-encrypted links or to find the best path in terms of latency while shedding battery-operated nodes constraint.

The graph built by RPL is a logical routing topology which is built over a physical network to meet some specific criteria.The network administrator may decide to have multiple routing topologies (graphs) simultaneously active which is used to carry traffic with different set of requirements. A node in the network can participate and join one or more graphs, and mark the traffic according to the graph characteristic to support Quality of Service awareness and constraint based routing. The traffic flows up and down along the edges of the specific graph.

IV. SYSTEM DESIGN AND IMPLEMENTATION

For the FIDO protocol ,a Java implementation open-sourced by eBay is used. The eBay implementation has the following main parts: a client module(Android), a server module (Apache Tomcat and Jersey) and a FIDO core module. An Open-TEE based

implementation can be added to the authenticator module from the FIDO core, in order to provide TPM solution which is hardware independent.

The FIDO registration process aims of having a trust relation between the users and the devices, by imprinting the device with the user's public FIDO key. The imprinting process does not involve the untrusted cloud entity. One important feature of this process is the fact that the registration is accountless, the user identity being preserved. In order to achieve this, the user authenticates to the IoT device with the attributes issued by the device manufacturer. These attributes can be peculiar for different applications and each attribute can activate different functions of the devices. For the attribute based authorization, CP-ABE (Ciphertext Policy Attribute Based Encryption) from the ACSC (Advanced Crypto Software Collection) implementation can be used. In this architecture, the device manufacturer sends to the user an attribute collection along with a private key. The private key is used to decrypt a nonce, generated by the device, in a FIDO registration challenge-response protocol.

The Administrator status and the subscription period are the attributes sent by the device makers. Once the FIDO registration is done, further user-to-IoT device authentication occur by employing the FIDO keys. The CP-ABE attributes are transported in the FIDO messages, for the solution to compy with FIDO. When the user application discovers the IoT devices' IP addresses, it browses a registration URL, which replies with a FIDO registration request message in return.The challenge field is produced by the IoT device. That will a random value in the FIDO protocol. The importance of the challenge field is that it presents a nonce which is encrypted using the attributes of administrators. By using this technique, the client module can decipher the challenge, using the CP-ABE private key issued by the device maker.

A. User Authentication

When the user wants a communication with the IoT device, it will send a JSON formatted command to the device through the cloud platform. After the reception of command message, the device will respond with a FIDO authentication request: header, challenge, transaction, policy. The transaction field is actually a representation of the original command message which triggered the authentication process. With the help of this technique, the user can verify that the device got a command message which is authenticated. In the authentication response message, the IoT device waits for a signature value calculated on top of a challenge and other fields.

B. Cloud Federated Authentication

The cloud federated authentication is another extension of the user authentication mechanism. This process also makes use of the FIDO authentication messages. The federated case is used when the cloud platform needs to process the IoT device data which requires the authorization by an user. When the cloud platform sends a JSON formatted command to the IoT device, the device will be processesing it and be sending a FIDO authentication request to the user. The cloud generated command is stored in the transaction field of the FIDO authentication request. If the user does the command authorization and verifies it to be legitimate , it responds to the IoT device with a FIDO authentication message. The device owner authorizes a cloud command, after witnessing the required actions on the smart-phone screen.

C. Theft Resistant Security Schemes

One important feature of a security scheme for smart-home IoT devices is the theft-resistant property. This paper studies about a theft-resistant scheme where a user can find if the IoT device which is given a command was removed forcefully from the smart-home environment.It solves the theft issue by implementing a feature using the conceptof siblings. Since this is inspired from[7],these siblings can be referred to as PICO siblings. In this scheme, a trust relation is created between multiple PICO devices, by making use of a K-out-of-n architecture. PICO proposes a protocol where keep-alive messages are exchanged between the siblings. If at least k-out-of-n siblings are reachable between each other , then the device will maintain a secret. Otherwise the device will remove a secret key, and will locki itself. Thus if the device is relocated after stealing ,the keep-alive protocols will be made to run and if that fails, the device will lock itself and it will not respond to any more commands from the user. This security architecture is based on the fact that it would be hard for an attacker to relocate all the smart-home device siblings with in a short time interval.

D. RPL

The RPL protocol is a distance-vector routing protocol based on IPv6.The RPL devices are interconnected according to a topology which combines mesh and tree topologies called Destination Oriented Directed Acyclic Graph(DODAG). A DODAG graph is constructed from a root node which is the data sink of the graph. There can be multiple roots configured in the system. The RPL

routing protocol specifies a set of new ICMPv6 control messages to exchange graph related information. DIS(DODAG Information Solicitation), DIO (DODAG Information Object) and DAO(DODAG Destination Advertisement Object) are the control messages for this purpose.

The DIO message is used by the root to advertise the information about the graph .The neighbouring nodes of the root will receive and process DIO message potentially from multiple nodes and makes a decision based on certain rules (according to the objective function, DAG characteristics, advertised path cost and potentially local policy) whether to join the graph or not. Once the node joined a graph it has a route toward the graph (DODAG) root. The graph root is called as the 'parent' of the node. The node computes the rank of itself within the graph, which can refer to the coordinates of the node in the graph hierarchy. If configured to act as a router, it starts giving out the graph information with the new information to its neighboring nodes. The node simply joins the graph and does not send any DIO message if it is a leaf node.The neighboring nodes do this process repeatedly and make parent selection, route addition and graph information advertisement using DIO messages. [16]

The DIS message is used by the nodes to transfer graph information from the neighboring nodes. It become active in a stable graph environment using the 'poll' or 'pull' model of retrieving graph information or in other conditions.[17] Similar to MP2P or 'up' direction of traffic, which flows from the leaf towards the root it is required that a traffic to flow in the opposite or 'down' direction. This traffic may start from outside the LLN network, at the root or at any intermediate nodes.

This asks the need for a routing state to be built at every node and a mechanism to populate these routes. This is accomplished by the DAO(Destination Advertisement Object) message. DAO messages are for referring prefix reachability towards the leaf nodes in support of the 'down' traffic. These messages transfer valid lifetime ,information regarding prefix and other information. Each joining of the graph sends DAO message to its parent set

V. EXPERIMENTAL RESULTS

For the evaluation of the authentication protocol studied in this paper, a simulation of smart-home network scenario is done. The delay caused by the running of this protocol by comparing to a scenario where normal security is aplied to the IoT cloud platform is evaluated. In a typical smart-home scenario there is a central node (typically the user with his smart-phone) which sends different commands to nodes (smart devices from home).

When using an IoT cloud platform, like Kaa IoT, the central node (controller) sends commands to the slave nodes.Thse commands can be unicast or broadcast messages.

A case is experimented where the controller sends a broadcast command to all the smart-home devices and the mean delay time is measured after the reception of messages by the devices.

Also the delay is computed after applying the fido protocol.

In connection with the implementation of the anti-theft security mechanism ,the Java based Californium library is used for implementing the CoAP communication.

For the anti-theft keep-alive mechanism, a challenge-response security protocol is checked based on HMAC and also a DTLS secure communication whic is having performance penalties similar to this.

Inorder to test RPL,the simulation model used in this work is based on the basic platform for the network simulator Cooja, which was designed as a simulator for IoT. Cooja is a simulator based on the Contiki OS using sensor nodes. It is an open source software, which is compatible with our requirements for this study.

Cooja offers the chance to simulate each node independently using hardware or software to our wish. It can operate at different levels:

network level, OS level, and the machine code instruction level. It can run on different platforms such as Sky, TelosB, native etc. .It is able to simulate each node separately too.

The flexibility of Cooja enables it to add some extensions in the simulator.

The main metric identified to evaluate our study is the Packet Delivery Ratio(PDR) which illustrates the level of data delivered to the destination. Better performance of the protocol provides greater value of PDR.

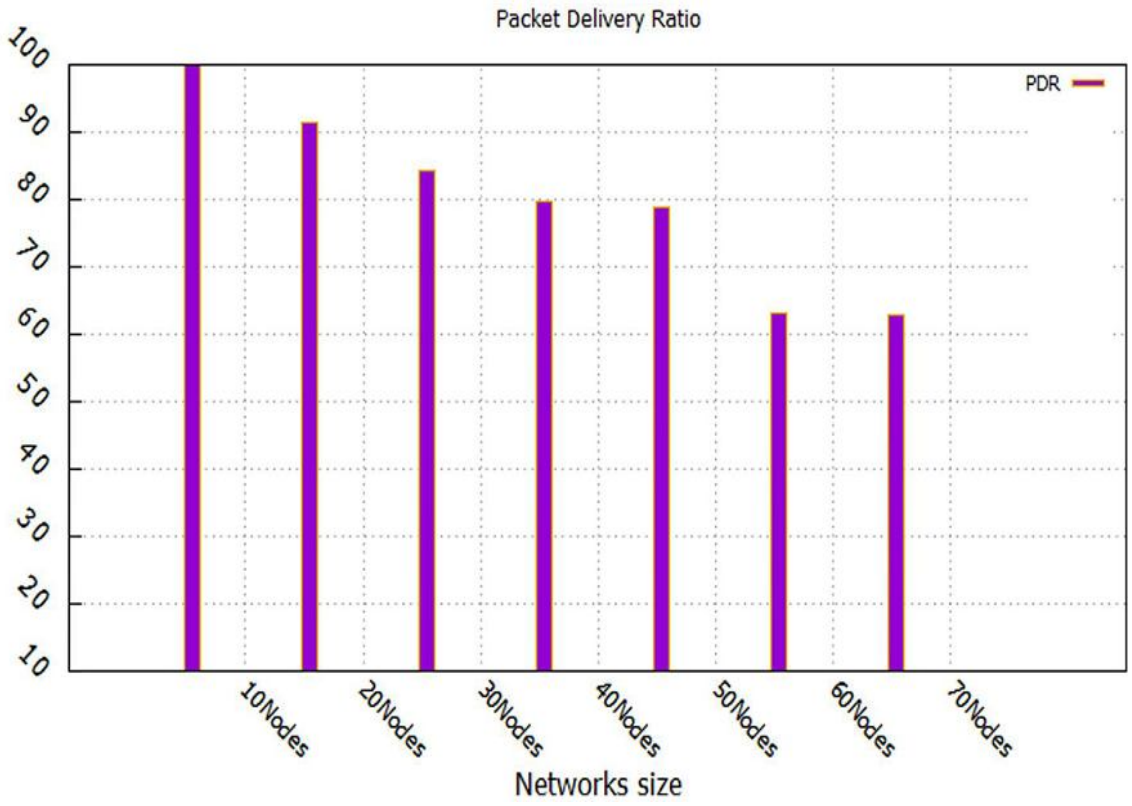


Fig 2 : Comparison of the Packet Delivery Ratio for different densities of networks [18]

Observations were made for local and global repair scenarios to see the time required during which no path was available. It was observed that in most of the cases the period of time without connectivity was less during local repair. These results were observed on particular networks for a given RPL parameters settings. It was observed that as the frequency interval is decreased the failure time gets also reduced at the cost of increase in control traffic. It was also observed that if the global repair interval was increased and the local repair was activated the failure time was reduced significantly while the control traffic increased slightly.

VI. CONCLUSION

In this paper,we studied about a security scheme for the users and devices of a smart home which are connected to an untrusted cloud entity. A proof-of-concept software solution which uses the FIDO protocol for users to authenticate to their devices is implemented. Moreover, a series of extensions and usages of the FIDO protocol is used, suitable for authorisation purposes. Also the protocol used preserves the user anonymity: manufacturers cannot create a linkage between different user accounts. This paper studies about a theft-resistant scheme as well where a user can detect if the IoT device which is issued a command was removed from the smart-home environment.

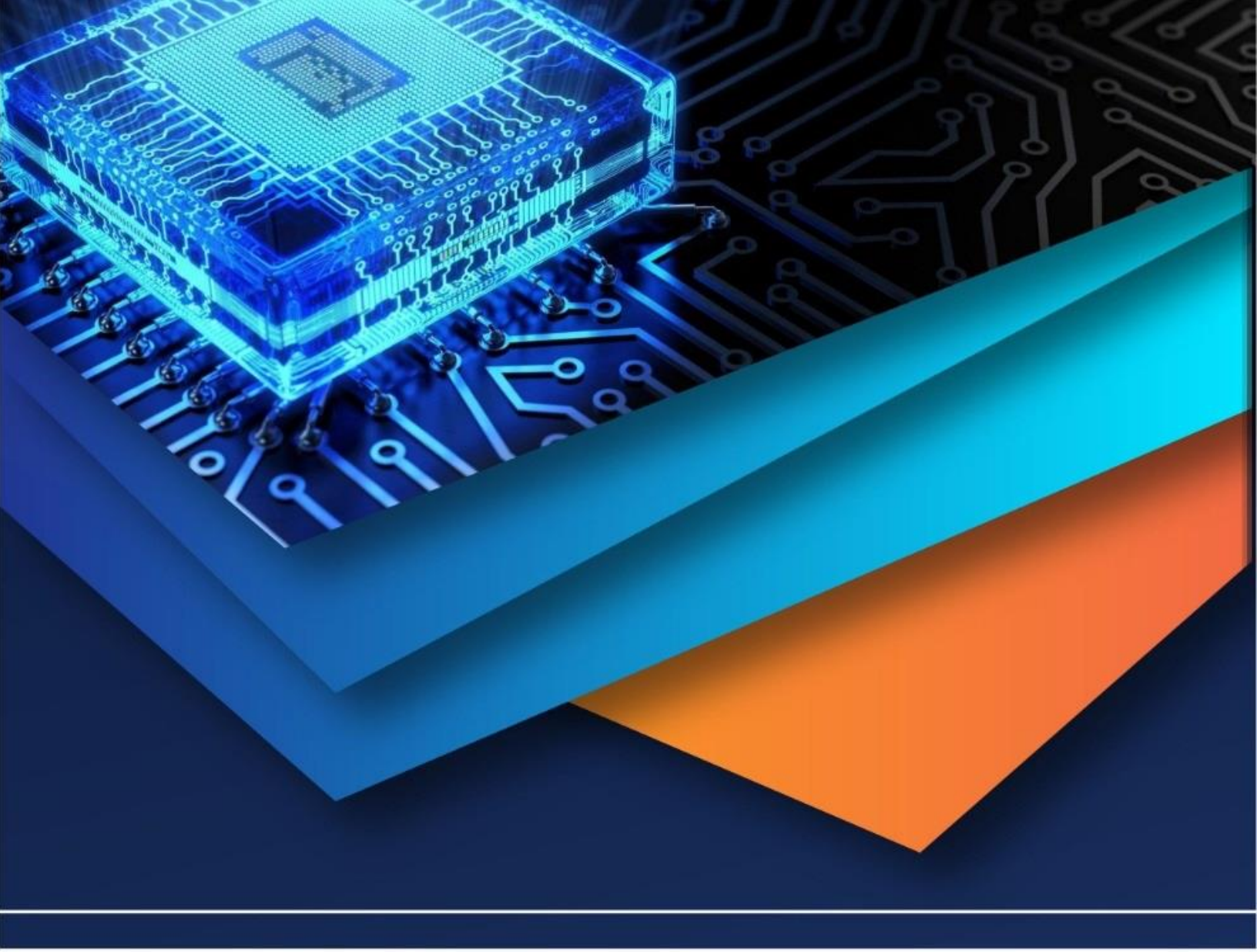
Assuming the communication is not reliable,a Routing Protocol for Low power and Lossy networks(RPL) is presented. It has the features: support of dynamic routing metrics and constraints,storing and non-storing nodes,loop avoidance and loop detection,global and local repair,timer management etc

Experimental results have shown that the additional delay introduced by the FIDO authentication protocol has a low impact for a smart-home appliation.Also,employing RPL helps in reducing loops in network and improving packet delivery ratio.

Low power and Lossy networks are emerging as an important part of ubiquitous computing and serving as a major building block for the communication infrastructure in the presence of IoT.However due to the shared radio medium, the lack of physical protection and security requirements of inherent routing protocol,low power and lossy networks are admittedly threatened by diverse Denial of Service attacks that primarily disrupt network protocols and interfere with on-going communications.So as a future work,an approach to mitigate these issues can be proposed.Also in future,the system can be redesigned and further improved by reducing the additional delays caused by the proposed protocols.

REFERENCES

[1] Bogdan-Cosmin Chifor, Ion Bica,Victor-Valeriu Patriciu, "A security authorization scheme for smart home Internet of Things devices" ,in Future Generation Computer Systems,2017,pp.167-192
[2] Jindou, Jia, Xiafeng, Qiu, Cheng,"Access control method for web of things based on role and sns.", In Computer and Information Technology (CIT),pp. 316-321, 2012.
[3] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC OJ L 257, 28.8.2014, pp. 73-114, 2014
[4] R. Lindemann, D. Baghdasaryan, E. Tiffany," Fido universal authentication framework protocol", Version v1. 0- rd-20140209, FIDO Alliance, February.
[5] H. Tschofenig, "Fixing user authentication for the internet of things (iot)",Datenschutz und Datensicherheit-DuD 40 (4) (2016) 222–224.
[6] M. Yoon, J. Baek, "A study on framework for developing secure iot service,"in: Advances in Computer Science and Ubiquitous Computing, Springer,2015, pp. 289–294.
[7] F. Stajano, Pico: No more passwords!, in: International Workshop on Security Protocols, Springer, 2011, pp. 49–81.
[8] Gubbi, J., Buyya, R., Marusic, S., and Palaniswami M. "Internet of Things (IoT): A vision, architectural elements, and future directions", Future Generation Computer Systems, 29(7), pp.16451660,2013
[9] Ndibanje, B., Lee, H. J., and Lee, S. G., "Security analysis and improvements of authentication and access control in the Internet of Things.", Sensors (Basel, Switzerland) 14(8), pp. 1478614805, 2011.
[10] A. F. A. Rahman, M. Daud, M. Z. Mohamad, "Securing sensor to cloud ecosystem using internet of things (iot) security framework", in: Proceedings of the International Conference on Internet of things and Cloud Computing,ACM, 2016, p. 79.
[11] Moghaddam, F. F., Moghaddam, S. G., and Rouzbeh, S.," A Scalable and Efficient User Authentication Scheme for Cloud Computing Environments", IEEE Region 10 Symposium, pp. 508-513, 2014.
[12] L. Barreto, A. Celesti, M. Villari, M. Fazio, A. Puliafito, "An authentication model for iot clouds", in: Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2015,ACM, 2015, pp. 1032–1035
[13] Tsai, J.-L., and Lo, N.-W., A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services,", IEEE Systems Journal, vol.9, no.3, pp. 805 - 815, 2015.
[14] Powell, C., Aizawa, T., and Munetomo, M., Design of an SSO Authentication Infrastructure for Heterogeneous Inter-cloud Environments,,IEEE 3rd international conference on cloud networking (CloudNet),pp.102- 107,2014.
[15] Qousini, A., Role-Based Access Control Model for Privacy Preservation in Cloud Computing Environment, Amman: The University of Jordan, 2015.
[16] IETF, "Rfc 6550: Rpl: Ipv6 routing protocol for low-power and lossynetworks," 2012.
[17] D. Gadde and M. Chaudhari, "Survey on routing protocol for low-power and lossy networks," in IEEE ICCIC Conference, 2015.
[18] Hanane Lamaazi , Nabil Benamar , Antonio J. Jara , "RPL-based networks in static and mobile environment: A performance assessment analysis",in Journal of King Saud University –Computer and Information Sciences,2017.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY