IJFEAT
INTERNATIONAL JOURNAL FOR ENGINEERING APPLICATIONS AND TECHNOLOGY

DESIGN AND DEVELOPMENT OF CONTEXT-AWARE SECURE ROUTING ARCHITECTURE IN INTERNET OF THINGS (IOT)

Mr. P. P. Lokulwar, Dr. H. R. Deshmukh
Department of Computer Science and Engineering , JDIET, Yavatmal, Maharashtra, India, prasad.lokulwar@rediffmail.com
Department of Computer Science and Engineering ,IBSS, Amravati, Maharashtra, India hrdphd@rediffmail.com

ABSTRACT:

Basically the Internet is a global system of interconnected computer networks. The original Internet architecture was not designed to meet current demands and the continuous strain in terms of sophisticated threats, performance, reliability, scalability and security. To overcome the problem of the current Internet specially focuses on the performance, reliability, scalability and security and despite the significant dropping price and increasing size of the storage. The amounts of data that are created today require ever-growing amounts of storage. However, data is not inherently associated with knowledge of their context. This information may be available at the communication end-points (applications) but not when data is in transit. So, it is not feasible to make efficient storage decisions that guarantee fast storage management, fast data mining and retrieval, refreshing and removal optimized for different types of data.

The lack of context-aware management is also closely related with the lack user and data privacy. In case we include data protection/encryption methods (even using asymmetric encryption and public key methods), data can't be efficiently stored/handled. On the other hand, lack of encryption, violates the user and data privacy. More investigations into the larger privacy and data-protection eco-system are required to overcome current limits of how current information systems deal with privacy and protection of information of users, and develop ways to better respect the needs and expectations.

In our thesis, we merge the fundamental concept of the context awareness computing model in Internet of Things and the routing protocol of the wireless sensor network, and proposes a new routing protocol CRP (Context based Routing Protocol) for Internet of Things, based on context-awareness which belongs to the key technologies of Internet of Things. Furthermore, our work describes the details on the protocol in the work flow, data structure and quantitative algorithm, context decision and reasoning algorithm and so on. Also proposed work, propose low complexity cryptographic algorithm for IoT and its attack detection analysis. Finally, the simulation is given to analyze the work performance of the protocol CRP. Theoretical analysis and experiment verify that CRP has higher energy efficient and longer lifetime than the congeneric protocols. The proposed work enriches the theoretical foundation and makes some contribution for wireless sensor network transiting to Internet of Things in this research phase

1 INTRODUCTION

The Internet of Things (IoT)

The Internet of Things (IoT) is a new paradigm that combines aspects and technologies coming from different approaches. Ubiquitous computing, pervasive computing, Internet Protocol, sensing technologies, communication technologies, and embedded devices are merged to build a system where the real and digital worlds meet and are continuously in a symbiotic intercommunication. The IoT vision is building the block of a smart object by putting intelligence into everyday objects; they turned into smart objects able not only to collect information from the environment and manage the physical world but also to be interconnected, to each other, through the Internet to exchange data and information. The expected massive amount of interconnected devices and the requisite amount of available data open new possibilities to build services that will bring tangible advantages to the society, environment, economy and individual citizens [1]. The following fig shows the definition of IoT.

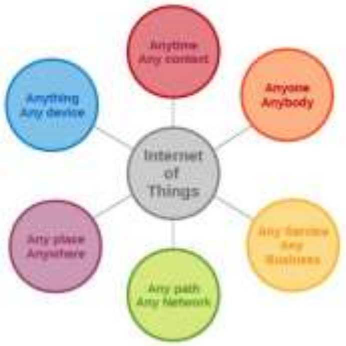


Figure 1: Definition of IoT

Context

1.6.1 A definition of context

According to the author [2][3], context is any data and that can describe the state of an entity and entity is any that is relevant to the interaction between a user and application. Context-Aware [2][3] Any system is context if it uses the context information and service related to the user and it also depends on the user's task. Gray and Salber (2001)[4] build upon this definition to derive a definition for sensed context, where they note that the notion of 'interaction' in the definition of context from Dey and Abowd is ambiguous. They arrive at the following definition:

Sensed context [4] Sensed context are properties that characterise a phenomenon, are detected and that are potentially relevant to the tasks supported by an application and the means by which those tasks performed.

Lieberman and Selker (2000) [4] take a broad definition from the side of application programming where they notice that traditionally the field of computer science has made the opposite position: the search for context-independence.

Their definition is as follows:

Context [5] Context can be considered to be everything that effects the computation except explicit input and output. These definitions help us to get a feeling of what context is. But also make clear that context is a broad concept. Dourish (2004)[6] says it like this: "'Context' is a slippery notion. Perhaps appropriately, it is a concept that keeps to the periphery, and slips away when one attempts to define it." Dourish in his article mainly objects against seeing context as something which is

independent of activity, and he has a point when he, for example, says that during a conversation the location of the conversation could turn from "context" to "content" when talking about it. In this report, we see the context in the broadest sense; everything which could be related to a specific event. As this is almost everything, when you read in this report about techniques for sensing, modelling and using context information, you should also be able to apply these techniques for sensing and modelling the world. What is essential in our definition is the word related which suggests that relating concepts is an important property of context.

Context Lifecycle

The lifecycle shows how the data move from phase to phase in a software system. It explains appropriately when the data is generated and data is absorbed and there is no longer limited to desktop, web, or mobile applications in context-awareness. Context awareness becomes the service Context-as-a-Service (CXaaS)[7]. Context management is an essential task in the software system, and this will grow in the IoT network.

The author[8] has classified the data lifecycle into two categories such as Enterprise Lifecycle Approaches (ELA) and Context Lifecycle Approaches (CLA) and in the Context lifecycle, WCXMS provide the context management information. Enterprise Lifecycle Approaches focus on only the context and it is well-established. Context Lifecycle Approaches is a contrast and it is not tested as compared to the Enterprise Lifecycle Approaches.

The author[9] explain regarding the life cycle recognised three stages in a typical context management system such as context acquisition, information processing, and reasoning and decision, some essential components shown in figure 2 [10][11].

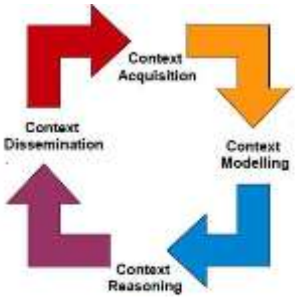


Figure 2: Context Life cycle

The context life cycle is divided into four steps, and these four steps are required for the context management system and middleware solution. The four phases are: First context acquisition, number of sources are available such as physical sensors or virtual sensors on that source it finds the context.

The data are collected need to represent according to the meaningful behaviour and it is the Second Step.

According to the modelled data is to derive high-level context data from low-level or i.e. raw sensor data and it is happening in the third step and finally, both high-level and low-level context requires being distributed to the consumers who are involved in context. The following discussion is based on these four phases.

1.7 Characteristics of context

1.7.1 Introduction

In this chapter, we will give an overview of the different characteristics of context information based on some previous work and own experience. With this overview, we hope to make clear where data management systems for use in AmI scenarios would differ standard data management systems. We tried to cluster the characteristics in three categories:

Acquiring Characteristics related to the acquisition of context.

User related Characteristics which focus on the demands of the user.

Consequences Characteristics which follow from the previous two.

2. SYSTEM ARCHITECTURE OF PROPOSE WORK

Internet of Things (IoT) is a network that is being used by wireless sensor connections and radio frequency identification (RFID) through wireless network and technology to achieve the overall perception of data, reliable transmission and intelligent processing. Hence preserving privacy and safety are the essential features of IOT [12]. This security is related to tag information (RFID), wireless communications information security, network transmission of information security, privacy and security information processing security. Therefore it is vital to have thorough study and research on design and improvement of security problems in IOT [13-14]. IOT consists of three layers: sensing layer, transport layer and application layer. The primary purpose of network security and information protection is to achieve confidentiality and integrity. Security issues are of great importance in enlarging the scale of network and devices [15-16]. There are some security risks in both consumers and business in IOT, so data encryption can be used to reduce security risks [17]. Hence we are providing a suitable Propose Low complexity Encryption Algorithm can play an effective role in reducing the security risks. The figure shows the general block diagram of propose encryption and decryption system[18].

3.1 Development of Context based Routing Protocol (CRP)

CRP is a distance vector routing protocol for IoT that makes use of ICMPv6. The term distance vector refers to the fact that the protocol manipulates vectors (arrays) of distances to other nodes in the network devices running the protocol are connected in such a way that no cycles are present. It is an Intra-domain routing protocol. It requires that a router inform its neighbours of topology changes periodically and have less computational complexity and message overhead. Distance-vector routing protocols are based on calculating the Direction and Distance to any link in a network[19]..

- "Direction" usually means the next hop address and the exit interface.
- "Distance" is a measure of the cost to reach a particular node.
- The least cost route between any two nodes is the route with minimum distance.
- Each node maintains a vector (table) of minimum distance to every node.
- The cost of reaching a destination is calculated using various route metrics

For this purpose, a Destination Oriented Directed Acyclic Graph (DODAG), which is routed at a particular destination, is built. The CRP term calls this specific node a DODAG root and the graph is constructed by the use of an Objective Function (OF) which determines how the routing metric is determined. In other words, the OF defines how routing limitations and other functions are taken into account during topology configuration. In unusual cases, a network has to be optimised for different application outlines and deployments. For illustration, a DODAG may be constructed in a way where the Expected Number of Transmissions (ETX) or where the current amount of battery power of a node is considered. For this reason, CRP allows building a logical routing topology over an existing physical infrastructure and context id. It specifies the so-called CRP Instance which defines an OF for a set of one or more DODAGs.

The protocol examines to avoid routing loops by computing a node's position relative to other nodes concerning the DODAG root. This position is called a Rank and improves if nodes go away from the root and decreases when nodes move in the other direction, respectively. The Rank may be equal to a fair hop-count distance, may be calculated as a function of the routing metric or it may be calculated concerning other constraints. The CRP specification defines four types of control messages for topology maintenance and information exchange. The first one is called DODAG Information Object (DIO) and is the primary source of routing control information. It may store information like the current Rank of a node, the current CRP Instance, the ICMPv6 address of the root, and so on. The second one is called a Destination Advertisement Object (DAO). It allows the support of down traffic and is used to generate destination data upwards along the DODAG. The third one is named DODAG Information Solicitation (DIS) and makes it possible for a node to require DIO messages from a reachable neighbour. The fourth type is a DAO-ACK and is assigned by a DAO recipient in response to a DAO message. The CRP specification defines all four types of control messages as ICMPv6 information messages with a requested type of 155. This new type has been officially confirmed by IANA [20]. Another important consideration about the protocol's design is the maintenance of the topology. Since most of the devices in a LAN are typically battery powered, it is essential to restrict the amount of sent control messages over the network. Several other routing protocols broadcast control packets at a fixed time interval which causes energy to be wasted when the network is in a stable condition.

The figure shows the DODAG root, and above the root, there is a context routing engine for processing of the fuzzification and defuzzification of the knowledge.

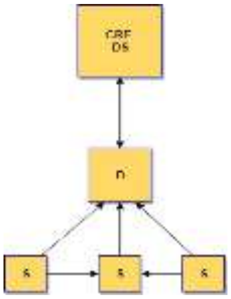


Figure 3: DODAG

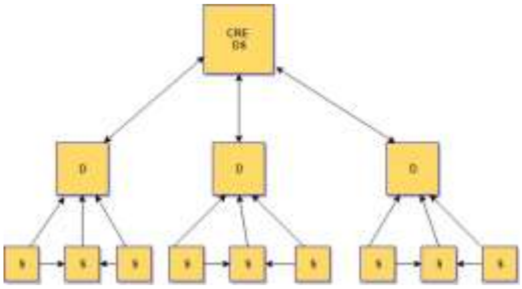


Figure 4: DAG

3.2 Development of Context Decision and Reasoning Model (CDRM)

The context reasoning model depends upon the fuzzification and defuzzification. Fuzzification is the process of changing a real scalar value into a fuzzy value. It is achieved with the different types of fuzzifiers (membership functions).

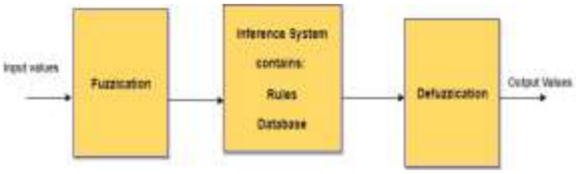


Figure 5: Context reasoning system

3.2.1 Fuzzy Inference System (FIS)

It is a method of determining the decision-making process with the help of some parameters human-like reasoning strategy, and it is achieved by defining the so-called linguistic variables; linguistic labels and membership functions [21]. It is realised using the fuzzy if-then rules that enable the linguistic statements to be treated mathematically. In this thesis, fuzzy inference system is applied to model the context uncertainty and incorporate a new source of knowledge using human rules, and it is used for device placements and indoor/outdoor environment detection.

3.2.2 Context Reasoning Using Fuzzy Inference System

The single source gathered the information is usually limited and may not be entirely reliable, accurate and complete. Hence we are focused on the multi-sensor data in a multi-level merging scheme to improve the accuracy and robustness of context-aware. The collected from the multi-sensors are combines for providing the better judgement, and it is the task of the multi-sensor fusion. It is one critical issue of the fusion is how this information can be integrated to produce more accurate outcomes, and it depends upon the three categories of the fusion such as sensor layer, fusion layer, decision layer [22]. Following figure 6 shows the multi-level sensor fusion pyramid along with the input.

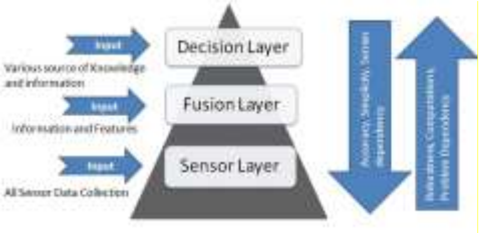


Figure 6: Multi-level sensor fusion pyramid.

The sensor layer it is also called as the low-level fusion it is the integration techniques work directly on the raw data obtained from the different sensors. Next, fusion layer it is also called the median-level fusion works on the extracted features which are available from different sources of information. The decision layer it is also called as the high-level fusion techniques that take place in the decisions and interpretations from different knowledge sources. Following table 13 shows the comparison of fusion techniques in different levels. There is no simple rule for selecting the proper fusion techniques.

The context reasoning is essential because it handles the ambiguity of the recognised activities, removes the conflicts, preserves consistency of detected context, fills the gaps, and fuse various sources of information [23]. It is defined in the form of the rules and then combines these rules using the decision level fusion algorithm may generate a more powerful understanding of the current situation. In this primary context is location, activity and the time and fusion of them at the decision level might generate valuable knowledge which acts a guide[24]. For example, knowing the current location and time, the system could have a pretty good idea of the user's current activity which can be used in context detection by adding association rules.

The determination of location and recognition of activities, high-level contexts are detected by incorporating association rules between the primary contexts in a reasoning engine. Then the decision level fusion fuzzy applied in context reasoning engine improves the efficiency of context and then context detection algorithm by applying new rules which are acquired from a various source of information such as existing context information, expert knowledge, user preferences or constraints. Figure 7 shows a decision level fusion fuzzy which integrates heterogeneous source of knowledge, information and sensors. It consists of context DB and context reasoning engines. It understands the gather contexts, checking the consistency and monitoring the context information and sensed and inferred context data could be converted to useful information according to the inference rules.

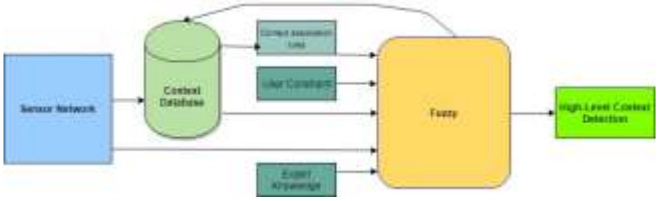


Figure 1: Context reasoning using fuzzy.

3.3 Development of Low Complexity Secured Context Routing Protocol for IoT in WSN environment (LCSCRP)

Lightweight cryptography[25] is a cryptographic algorithm tailored for implementation in constrained environments including RFID tags, sensors, contactless smart cards, health-care devices and so on. In hardware implementations, chip size and energy consumption are the critical measures to evaluate the lightweight properties. In software implementations, the smaller code and RAM size are preferable for the lightweight applications. The implementation properties, the lightweight primitives are superior to conventional cryptographic ones. Lightweight cryptography also delivers adequate security. Lightweight cryptography does not always exploit the security-efficiency trade-offs. The report of recent technologies of lightweight cryptographic primitives. Nowadays, in the area of a lightweight block cipher, some of the lightweight block ciphers are proposed, such as PRESENT, LBlock, TWINE, KLEIN, MIBS, LED, PRINCE, Piccolo, ITUbee, EPCBC, PRINT cipher and RECT- ANGLE[26]. Structures of these lightweight ciphers as like traditional block ciphers are generally developed into two main classical structures: SPNs and Feistel-type structures.

The SPN structure[27] is developed using round function on the entire data block. The slow diffusion of the conventional Feistel- type structures has some security problems. Consequently, to solve these problems the ciphers in traditional Feistel-type structures many rounds in contrast to the ciphers based on SPNs is needed; thus, this increases energy consumption. Nevertheless, compared to SPNs, the traditional Feistel-type structures have more features.

- It has a small and simple round function.
- It has the same program for encryption and decryption processes to reduce decryption implementation cost.

Why is lightweight cryptography needed for IoT? "Lightweight Cryptography", in the IoT needed for two reasons[28]:

1. Reliability of end-to-end communication: In order to achieve end-to-end security, end nodes have an implementation of a symmetric key algorithm. For the low resource-devices, e.g. battery-powered devices, the cryptographic operation with a limited amount of energy consumption is important.

2. Applicability to lower resource devices: The lightweight cryptographic primitives are smaller than the conventional cryptographic ones. The lightweight cryptographic primitives would open possibilities of more network connections with lower resource devices. However, lowest cost devices can embed only application-specific ICs due to limited cost and power consumption, where hardware properties are crucially important.

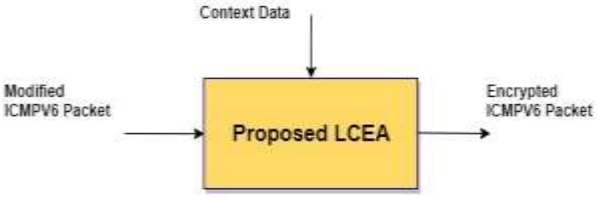


Figure 8: General Block Diagram of Encryption System

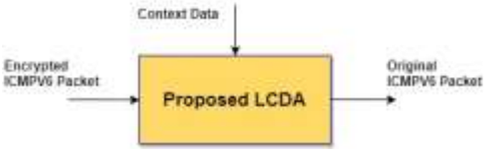


Figure 9: General Block Diagram of Encryption System

Following diagrams show the proposed block diagram of the encryption and decryption system of the Low complexity Context Routing Protocol.

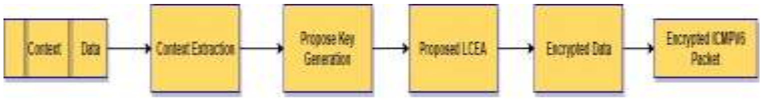


Figure 2: Proposed Block diagram of Encryption System

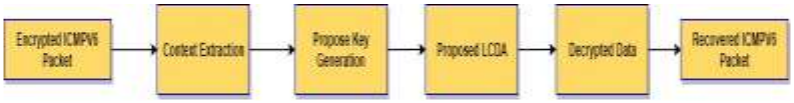


Figure 11: Proposed Block diagram of Decryption System

3.4 Development of Attack Resistance System in WSN (ARS)

Internet of things (IoT) that combine a variation of devices into networks to provide advanced and intelligent services should protect user privacy and address attacks such as spoofing attacks, denial of service attacks, man middle in attack jamming and eavesdropping[29]. Consisting of the things, services, and networks, IoT systems are unprotected to network attacks, physical attacks, software attacks and privacy leakage. In this article, we focus on the IoT security threats as follows.

• DoS attackers aim to prevent IoT devices from receiving the network and computation resources [30].

• DDoS attackers with thousands of IP addresses make it more difficult to distinguish the legitimate IoT device traffic from attack traffic. Distributed IoT devices with light-weight security protocols are especially vulnerable to DDoS attacks [31].

• Jamming attackers send faked signals to interrupt the ongoing radio transmissions of IoT devices and further deplete their bandwidth, energy, central processing units (CPUs) and memory resources of IoT devices or sensors during their failed communication attempts [32].

• Spoofing: A spoofing node impersonates a legal IoT device with its identities such as the medium access control (MAC) address and RFID tag to gain illegal access to the IoT system and can further launch attacks such as DoS and man-in-the-middle attacks [33].

• Man-in-the-middle attack: A Man-in-the-middle attacker sends jamming and spoofing signals with the goal of secretly monitoring, eavesdropping and altering the private communication between IoT devices [30].

• Software attacks: Mobile malware such as Trojans, worms, and the virus can result in the privacy leakage, economic loss, power depletion and network performance degradation of IoT systems [34].

• Privacy leakage: IoT systems have to defend user privacy during the data caching and exchange. Some caching owners are curious about the data contents stored on their devices and analyse and sell such IoT privacy information. Wearable devices that collect user's personal information such as location and health information have witnessed an increased risk of personal privacy leakage [35].

3. RESULT AND DISCUSSION

6.1 A PC with specifications:

2.40GHz processor Intel i3 and 3GB RAM is used as the work station.

Performance Parameter Evaluation

In this thesis, design the virtual environment of the simulation in Matlab based on the physical equipment.

6.2 Design and Develop the proposed CBRP (Context Base Routing Protocol)

In the Propose Context Base Routing Protocol i.e. CBRP node in the network are divide into cluster area on the basis of the filed dimension, numbers of node in the field and the number of rounds. In the cluster area decide the one cluster head on the basis of the energy and threshold value or node which is nearer to the base station and every time the cluster head is change. The following figure shows the Context Base Routing Protocol i.e. CBRP.

- **Better Addressing Method**

If the device identity privacy is not addressed then it can lead to following risks:

- Device can be associated with wrong identity information and result into confusion.
- Device identity information can be out of date and in this case device cannot communicate any more.
- Identity information of devices can be proclaimed by unauthorized party or device.
- Misuse of device identity information by someone other than its authorized owner.

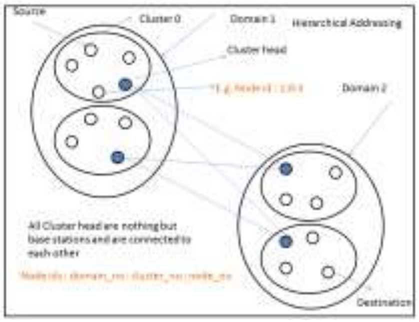

Source
Cluster 0
Domain 1
Hierarchical Addressing
Cluster head
Domain 2
All Cluster head are nothing but base stations and are connected to each other
Destination

Figure 12: Example Clustering Scenario in CCHA

The **Simulation Scenario:**

The simulation in this contribution is conducted using MATLAB. The simulation is carried out to measure the following two sets of parameters. The simulation environment is shown below in the Table 1.

Table 1: Simulation Parameters for CBRP

Sr. No	Parameter	Value
1	Number of Nodes	50-200
2	No of rounds (can specified in time)	100
3	Area Coverage (in meter)	100m x 100m
4	Source Voltage	3 - 4V (DC)
5	Transmitting current	30mA
6	Transmitting Power	+0.5dBm
7	Reception Power	+0.5dBm
8	Receiving current	37mA
9	Single Hop Distance (Line of sight dist)	150m
10	Antenna Type	Omni Directional
11	Power Supply capacity/node	60mAh
12	Time Slice	60s (can vary
13	Data rate of node	250Kb/s (can vary)

The following figure 75 shows the propose Context Base Routing Protocol and it is base on the some parameters such as field of the dimension or size of the network, number of the nodes are present in the field and the important thing is that he number of rounds because energy of the nodes which is depend on the rounds. If the number of rounds in minimum consumption of the energy and if the rounds in maximum then more energy is used then the node is dead.

Divide the network according to the field, number of nodes in the field and number of rounds which is shown in the following figure 13.

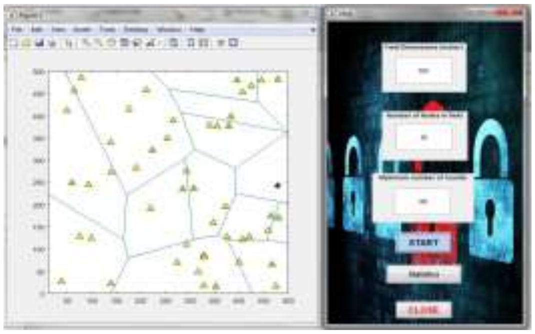


Figure 13: Divide the network into cluster

Evaluation Results

The evaluation result shows the average energy of the each node and number of the dead node is possible during the process. The following figure 14 and figure 15 shows the average energy of the each node and number of the dead node.

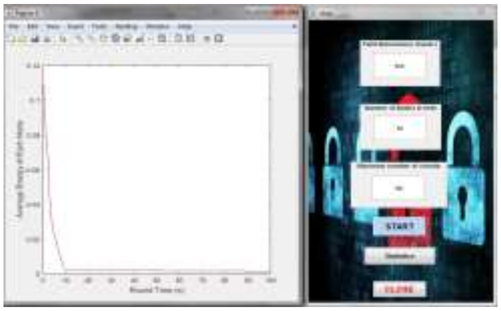


Figure 14: Average energy of each node

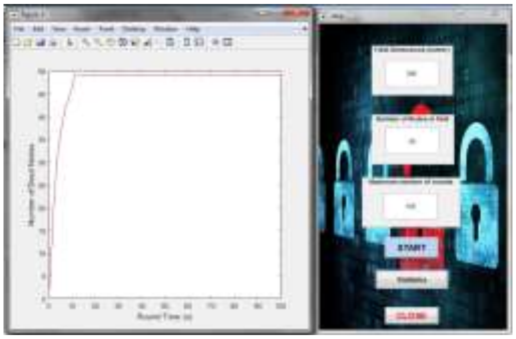


Figure 15: Number of Dead Node

The following figure 16show the statistic of the context Base Routing Protocol with calculating the total execution time in seconds, initial number of the dead node, After time slice how much node are dead and how much packets are delivered i.e. average packet delivery ratio.

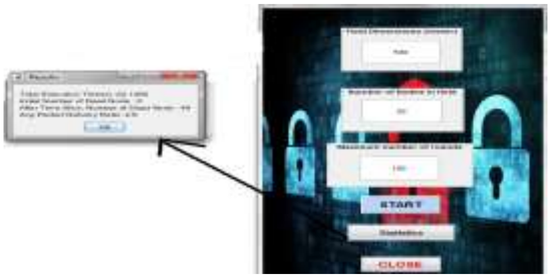


Figure 16: Statistic of the CBRP

6.3 For Context Awareness (classification and decision) Model

Efficient Context Management scheme for device Classification

Devices are classified based on their geographical positions and this contextual information is used for event detection. In this approach, a complete match is carried out to fetch device type and provider from the database. Reliability is not proved with even the proof of concept in this approach. Communication cost in terms of energy, PDR is also not addressed in and the time analysis is based on the statistical data which is not appropriate approach in the context of IoT. Even the results the proposed are encouraging; it has not been possible to validate the capability of the proposed approach in actual test bed with multi-technology sensor nodes. The Following Figure 80 shows the Propose framework for Device classification.

Evaluation Result:

The below figure 81 shows the different scenario such as Office, home according to the scenario we are set the values and reasoning are done with the help of the Fuzzy inference system and rules of the FIS system.

The result is shown in below figure 17 with the help of the confusion matrix and in the confusion matrix value is calculated in the diagonal view it means that blue box it is the output value of the matrix.

Figure 17: Analysis with the help of the Confusion Matrix

The following figure 18 shows fuzzy inference system are use the member function for the different parameters such as the temperature, distance, pressure, luminance and time.

Figure 18: Fuzzy Inference System

Following table 2shows the summary of the result with the help of the different parameters.

Table 2: Result of all parameters (%)

The following table show the result of the different parameters with the help of the confusion matrix.

Parameters	**AC**	**TP**	**FP**	**TN**	**FN**	**ER**	**P**	**SN or Recall**	**SP**	**F-mea**
Values	90%	100	0.0	80	20	10%	100%	83.33	100	96.1538

6.4 For routing protocol

Evaluation Parameters:

In below figure, **square represent conventional LEACH** protocol results and **triangle represent proposed CBRP**.

For this scenario assumptions considered Area = 100m x 100mNo of sensor nodes = 200

In the following figure Red Line shows the result of the Leach Protocol and Green Line is shows the result of the propose CBRP.

Evaluation Results:

The following figure 19 and 20 shows the comparison between the LEACH protocol and propose CBRP with the help of the showing the result of the average energy of each node and number of the dead node with respect to the number of the rounds.

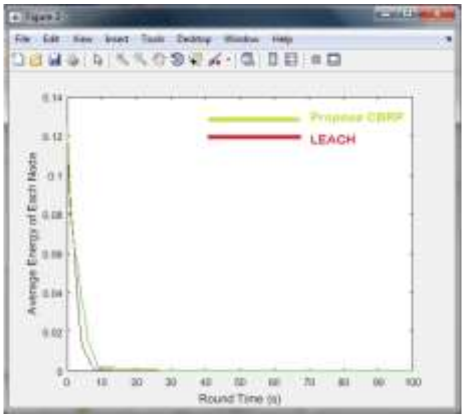


Figure 19: Average energy of each node vs. number of round

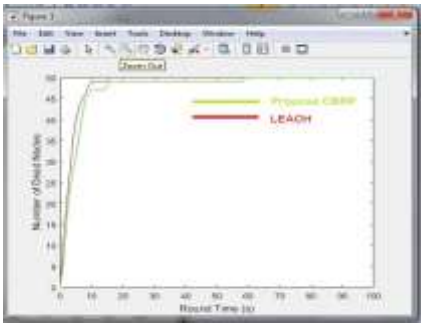


Figure 20: Number of dead nodes vs. number of round

End to End Delay:

The following table 3 shows the result of the end to end delay in second and also shows the propose CBRP is best result as compare to the LEACH protocol and propose CBRP is efficient for Internet of Things .

Table 3 Show the result of end to end delay

No of Rounds	End to End Delay (s)	
	LEACH	Proposed
100	5.1	3.58

Throughput:

The following table 4 shows the result of throughput in second and also shows the propose CBRP is best result as compare to the LEACH protocol and propose CBRP is efficient for Internet of Things . The propose CBRP having more threshold factor i.e. number of process executed per unit time is more as compare to the LEACH.

Table 4: Show the result of throughput

Throughput (packet per msec)	
LEACH	Proposed
62	128

Packet Delivery Ration (PDR)

The following table 5 shows the result of Packet Delivery ratio and also shows the propose CBRP is best result as compare to the LEACH protocol and propose CBRP is efficient for Internet of Things . The propose CBRP having more packets deliver as compare to the LEACH.

Table 5: Show the result of packet delivery ratio

No of Rounds	Packet Delivery Ratio	
	LEACH	Proposed
100	0.31	0.71

6.5 For Low Complexity Encryption and Decryption Algorithm system (Secure CBRP)

The simulation of the algorithm is done to perform the standard tests MATLAB R2016a. To test the security strength of the proposed algorithm, the algorithm is evaluated on the basis of the following criterion. Key sensitivity. We further tested the algorithm for computational resource utilization and computational complexity. For this we observe the memory utilization and total computational time utilized by the algorithm for the key generation, encryption and decryption.

Secure Context Base Routing Protocol

IoT security requirements to counter the threats like tampering, fabrication and theft of resources are listed below:

1. **Access control**

The access control provides authorized access to network resources. IoT is ad-hoc, and dynamic in nature. Efficient and a robust mechanism of secure access to resources must be deployed with distributed nature.

2. Authentication

Authentication is an identity establishment between communicating parties (devices). Due to diversity of devices, and end users, there should be an attack resistant and lightweight solution for authentication.

3. Data confidentiality

Data confidentiality is protecting data from unauthorized disclosure and data tampering. Secure, lightweight, and efficient key exchange mechanism is required due to dynamic network topology.

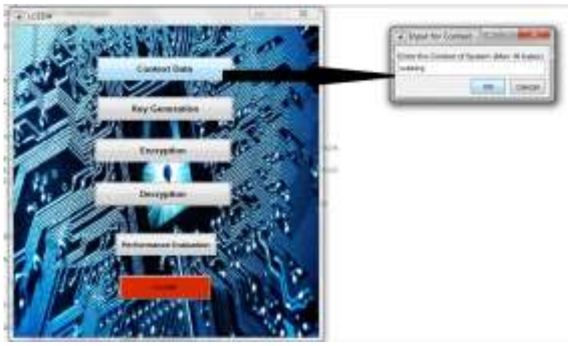
4. Availability

Availability is ensuring no denial of authorized access to network resources. Access control and availability problems are critical due to the wireless nature of ad-hoc networks.

5. Trust Management

Trust management, and trust-based access control are basic requirements in IoT due to its nomadic nature. Decision rules needs to be evolved for trust management in IoT. The secure routing protocol is depend upon the context data the following figure shows the LCEDA i.e. Low Complexity Encryption and Decryption Algorithm and the following figure 87 shows the Propose block diagram of the low complexity encryption and decryption algorithm.

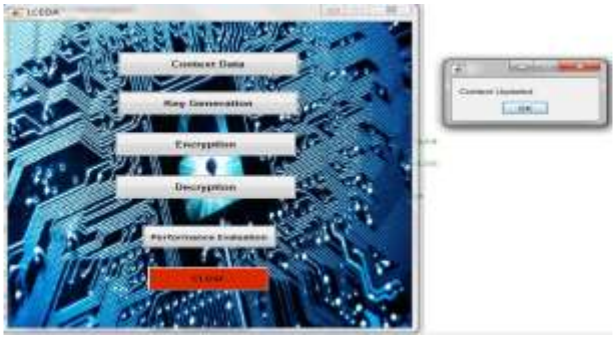
The below figure 21 shows the steps of the low complexity encryption and decryption algorithm or the system and getting the context data from the packet having the length of the context data at max 16 bytes.



Enter the Context of System (Max 16 bytes)

Figure 21: Enter the Context Data

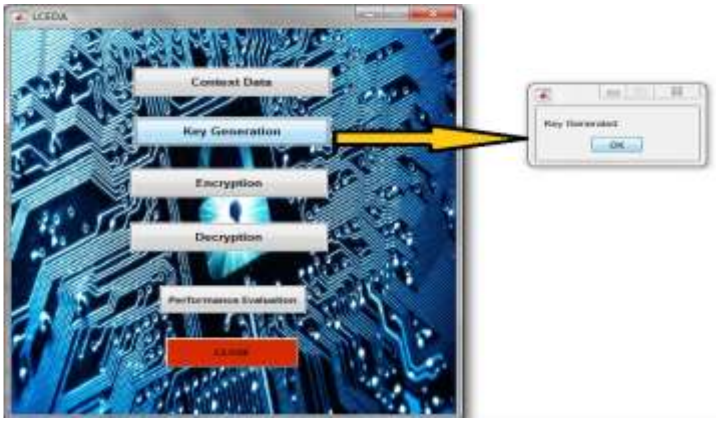
The Context data is uploaded successfully which is shown in the below figure 22.



Context Uploaded

Figure 22: After Enter the Context data Uploaded

After the Context Data is uploaded the next is the Key Generation and the key is generating on the basis of the context. The following figure 23 shows the Key Generation.



Key Generated

Figure 23: Key Generation with the help of the Context Data

The following figure 24 shows the encryption and decryption of the data with the help of the encryption and decryption algorithm.

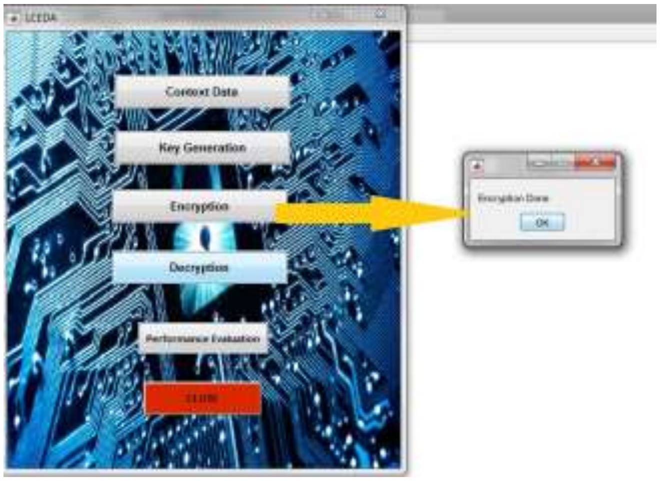


Figure 24: Encryption **of** data from ICMPv6 Packet

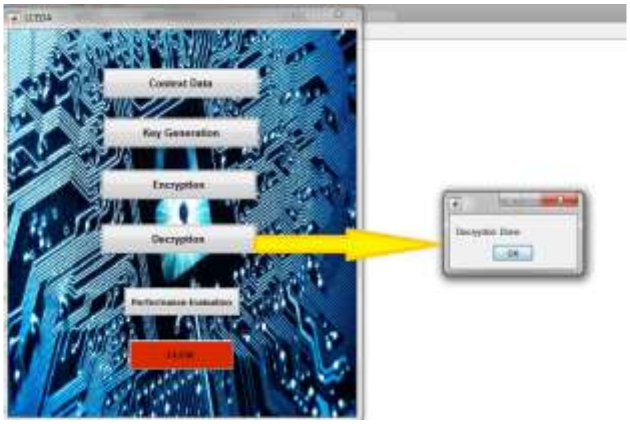


Figure 25: Decryption of data from ICMPv6 Packet

The following figure 26 shows the performance evaluation of the Low Complexity Encryption and Decryption Algorithm with the help of the calculating the encryption time, Decryption time, Elapsed time for key generation and the last is the Throughput.

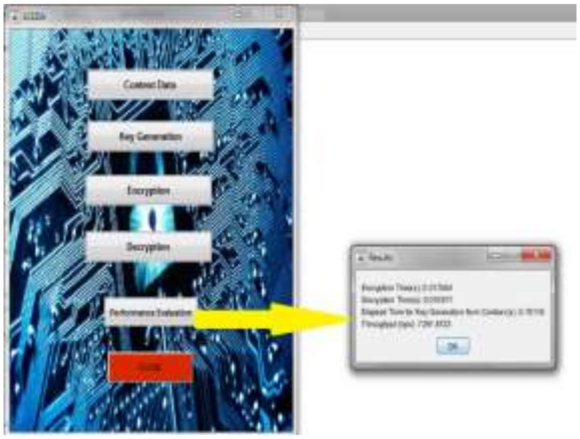


Figure 26: Low Complexity Encryption and Decryption Algorithm

Table 6: Parameters of encryption and decryption system

No of Bits	Block Size	Key Size	ET (ENC) s	DT(ENC) s	Throughput kbps
128	16	32	0.01754	0.010917	7291.8723

6.6 Improved Trust Management

There are three types of trust via:

a) **Interpersonal** trust represents entity-based, and context specific trust.

b) **Structural** trust represents a system within which the trust exists.

c) **Dispositional** trust represents a trust which is independent of entity, and context.

There are different trust management approaches and generic trust management life cycle is shown in the Figure 4.1. In a nutshell, any trust management model comprises of four phases of trust calculations as:

- Negotiation – Trust establishment between new devices
- Collection – Collecting trust scores of individual device in IoT
- Evaluation – Deals with the trust evaluation based on some fuzzy, or non-fuzzy rules,and some evaluation policies
- Propagation – Transfer of trust score to other devices, and in turn delegating other details like access rights etc.

The trust is defined as a subjective and context-based value which presents probability prediction of device to other device's behavior. Trust is a fuzzy parameter which is dynamic, and non-monotonic. In uncertain environments like IoT, fuzzy approach for trust calculations is more appropriate to quantify, and evaluate device behavior, and in turn access control rules.

6.7 For Attack Resistance System

This section discusses the results obtained from the proposed algorithm using MATLAB. It is a 4th generation high level programming language developed by Math Works. It provides an interactive environment for numerical computation, visualization, iterative exploration, and programming.

This is the part where the proposed solution is tested to check whether it is effective. The system was evaluated by use of network traffic traces of denial of service attacks which were collected from CAIDA and UCLA trace dataset. The evaluation is a three step process that involves: firstly, capturing of packets by use of a Linux-based packet sniffer, secondly calculation of an IP feature table from different sources and thirdly, it involved the use of the training of the neural network algorithm for testing the system.

Attack Dataset

The first Dataset is obtained from University of California, San Diego data center for Applied Internet Data Analysis (CAIDA). This acquired data is a length of one-hour packet capture of a distrusted denial-of-service attack which targeted a server to block its legitimate user from access. It overwhelms the entire network bandwidth. It contains about 360 million sniffed packet which is too large to deal with. Therefore, two million spoofed packets have been extracted randomly to conduct this experiment.

Normal Dataset

The second dataset is obtained from University of California, Los Angeles, Laboratory for Advanced Systems Research. This obtained data is a length of 5 minutes' packet capture of normal use from the border router of UCLA Computer Science Department. It contains around 265 thousand capture packets. To mirror the attack dataset, selected packets within the time window of the attack dataset have been chosen.

The attack detection and classification is based on the Learning and Testing which is shown on the following figure.

Learning:

It is an application of artificial intelligence and it provides the system or ability to automatically learn. It also improves from the experience. It uses the data and it learns from themselves and the process of the learning start with the observations or data such as examples, direct experience or the instruction.

The below figure 27 shows the GUI of the attack detection and classification of the proposed system with the help of the machine learning and it is divided into the learning and testing system and SVM.

Firstly load the database in the learning system because there are two types of the learning supervised learning and unsupervised learning. The output is known it is called as the supervised learning and which is shown in the following figure 96.

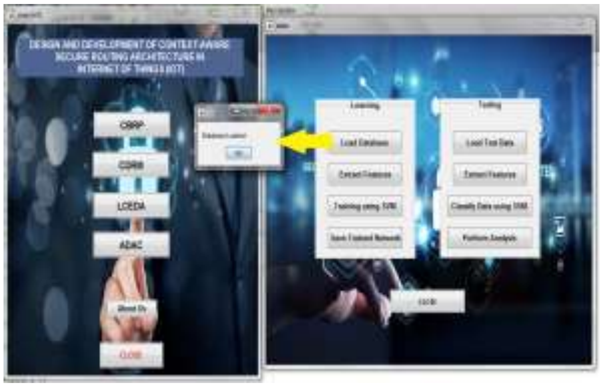


Figure 27: Load Database

Feature extraction involves reducing the amount of resources required to describe a large set of data. When performing analysis of complex data one of the major problems stems from the number of variables involved. The following figure 28 shows the feature extraction.

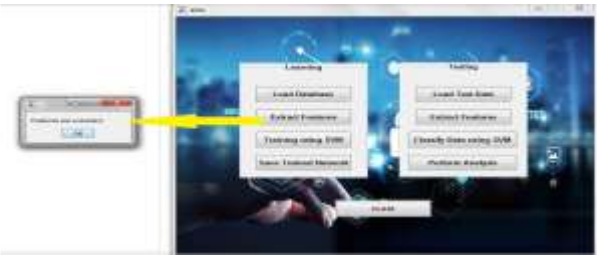


Figure 28: Extract Features of the Learning

The training data set is used for the training of your machine learning model and which is shown in the following figure 29.

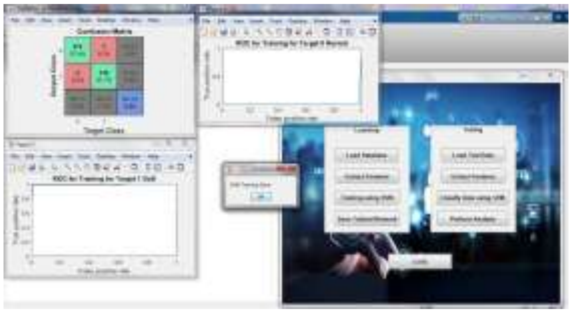


Figure 29: Training using SVM

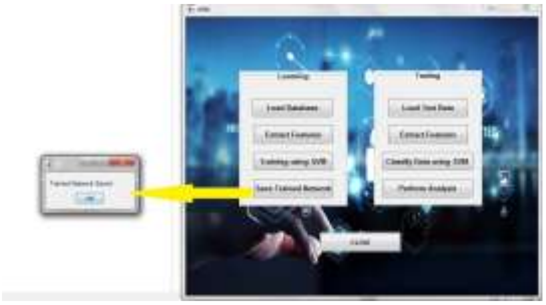


Figure 30: Trained Network Save

Testing

This is a subset of the training dataset that is intelligently built to test all the possible combinations and estimates how well your model is trained. The model will be fine-tuned based on the results of the test data set.

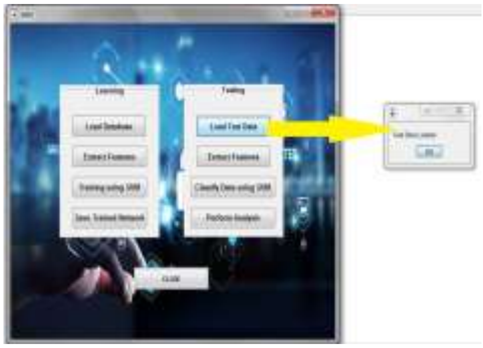


Figure 31: Load Test Data

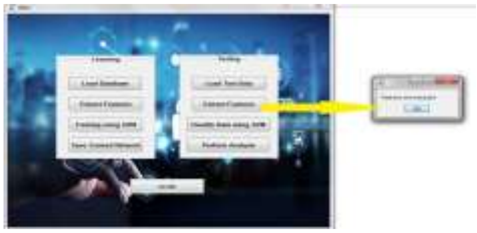


Figure 32: Extract Features of the Testing

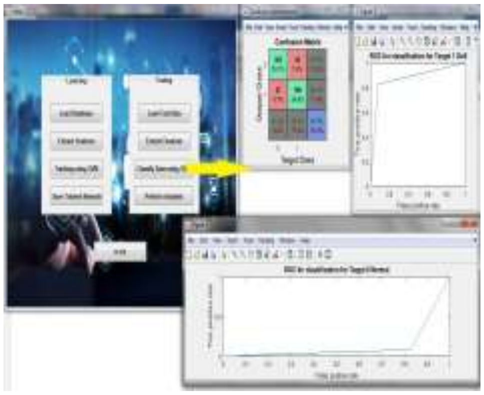


Figure 33: Classify the data using Support Vector Machine

The following perform the analysis of the with the help of the total evaluation time, accuracy, true positive rate, false negative rate, true negative rate, false positive rate, error rate, precision, recall, sensitivity, specificity and F-Score.

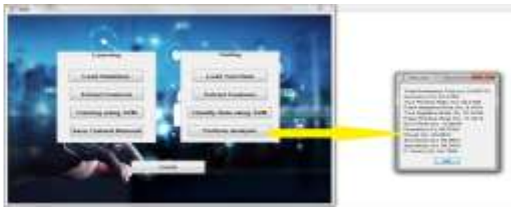


Figure 34: Attack Detection and Classification

The following table 7 illustrates the information of the used datasets.

Parameters/Method	Precision	TPR	F-score	FPR	FNR
Proposed (%)	82.57	82.57	84.12	17.42	8.1818

Table 7: Information of the used datasets

Stronger Access Control Scheme

This use case and misuse case clearly depicts the how the smart home is prone to attack for access control operations. There are several use cases possible for different scenario cases. In the sequel, different threat collected and control objectives are summarized below:

a) Access rights granted to unauthorized entity

Access rights may be granted to an unauthorized actor if an attacker is able to subvert the access control process. One way to do this may be done through impersonation, social engineering, by sending targeted e-mails requesting for access rights etc.

* Access rights should only be granted to actors after verification of their identity.

* Provision of filters or other equivalent mechanism should be installed to identify type of actors.

* If no formal verification of identity possible, then should be alert provision before granting access rights.

b) Corruption of access credentials

Depending on the chosen solution used for representing access right credentials, attacker is able to get hold of certain options. If the credentials are stored with the device they may be subject to manipulation by a malicious entity (user / device). This can be used to gain extra privileges by tampering with the credential's data structure.

* A secure design should be used to implement credential storage. Credentials should be stored on a device or should be generated depending on the context, to avoid tampering by an attacker.

Otherwise integrity of credentials should be protected by cryptographic means.

c) Unauthorized data transmission

Unauthorized data sent by an entity of an IoT network may lead to a breach of privacy.

Even the number or the different types of devices constitute private data.

- Traffic monitoring should be detected.
- Integrity of messages should be taken care

d) Denial of Service (Dos) attack

If a successful DoS attack can be mounted against the smart door software agent or then notification alerts about the door open status can be suppressed. If this attack is combined with the first one then access to the Smart Home can be obtained.

* Software agent should be proofed against tampering and DoS attacks.

e) Man-in-the-middle attack

Federation over insecure network may lead to eavesdropping which may be exploited further for data theft or identity theft.

* Federation requests should only be accepted from entities after verification of their identity.

*Strong encryption techniques should be employed to protect confidentiality of identity or location to ensure identity/location privacy.

A threat analysis presented may also comprise a risk analysis where severity and probability can be estimated and then risk can calculated for each threat. The objective of this use case and misuse case-based threat modeling is to incorporate them in the security assessment of IoT networks.

4. CONCLUSION AND FUTURE SCOPE

In an IoT network, nodes have the stronger sensory ability and smarter intelligence. So in this project we propose the protocol Context Routing Protocol (CRP) as the representative which using the core idea of the context-aware computing into the basic routing protocol. The context information will become more critical, and security is the main challenges with the development of IoT, because we will not satisfy by gathering the data, but knowing the meaning of the data.

Based on the conventional computing model as discussed in above chapter, we transform the traditional routing thought into a predictable routing protocol with using fuzzy match theory of artificial intelligence and Markov probability model, which contain some forwarding and directive meaning. It is an exploratory evolution direction of the WSN technology by the IoT guidance feature in the future. Through the simulation and analysis of CRP, the results show that the CRP has a longer lifetime and lower energy consumption, which indicated that CRP is more suitable for the IoT routing based on conventional computing model.

However, it still has abundant space for improvement and the core protocol CRP proposed here can be improved continuously by the theory circles as a fundamental protocol framework, and can also be enhanced to a cluster-type protocol. We will keep on researching this field.

REFERENCES

[1] B. Schilit and M. Theimer, “Disseminating active map information to mobile hosts,” Network, IEEE, vol. 8, no. 5, pp. 22 –32, sep/oct 1994. [Online]. Available: http://dx.doi.org/10.1109/65.313011

[2] Dey, A. K. and G. D. Abowd (1999). Towards a better understanding of context and context-awareness. Technical report GIT-GVU-99-22, Georgia Institute of Technology.

[3] Dey, A. K., G. D. Abowd, and D. Salber (1999). A context-based infrastructurefor smart environments. In 1 st Intl. Workshop on Managing Interactions in Smart Environments (MANSE’99).

[4]Gray, P. D. and D. Salber (2001). Modelling and using sensed context information in the design of interactive applications. In Proceedings of the 8th IFIP International Conference on Engineering for Human-Computer Interaction, pp. 317–335. Springer-Verlag.

[5] Lieberman, H. and T. Selker (2000). Out of context: computer systems thatadapt to, and learn from, context. IBM Systems Journal 39 (3-4), 617–632.

[6]Dourish, P. (2004). What we talk about when we talk about context. Personal Ubiquitous Comput. 8 (1), 19–30.

[7] G. Hynes, V. Reynolds, and M. Hauswirth, “A context lifecycle for web-based context management services,” in Smart Sensing and Context, ser. Lecture Notes in Computer Science, P. Barnaghi, K. Moessner, M. Presser, and S. Meissner, Eds. Springer Berlin / Heidelberg, 2009, vol. 5741, pp. 51–65. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-04471-7 5

[8] S. Yanwei, Z. Guangzhou, and P. Haitao, “Research on the context model of intelligent interaction system in the internet of things,” in IT in Medicine and Education (ITME), 2011 International Symposium on, vol. 2, dec. 2011, pp. 379 –382. [Online]. Available: http://dx.doi.org/10.1109/ITiME.2011.6132129

[9] A. Bernardos, P. Tarrio, and J. Casar, “A data fusion framework for context-aware mobile services,” in Multisensor Fusion and Integration for Intelligent Systems, 2008. MFI 2008. IEEE International Conference on, aug. 2008, pp. 606 –613. [Online]. Available: http://dx.doi.org/10.1109/MFI.2008.4648011

[10] Ephrem, E. (2015, June 8). Architecture of Wireless Sensor Networks. Retrieved October 8, 2015, from http://servforu.blogspot.com.tr/2012/12/architecture-of-wirelesssensor networks.html

[11] G. Chen and D. Kotz, “A survey of context-aware mobile computing research,” Department of Computer Science, Dartmouth College, Hanover, NH, USA, Tech. Rep., 2000, http://www.cs.dartmouth.edu/ reports/TR2000-381.pdf [Accessed on: 2011-12-05].

[12] W.Bruce D, GR. Milne, YG.Andonova, and F M. Hajjat. "Internet of Things: Convenience vs. privacy and secrecy." Business Horizons 58, no.6, Science Direct, p.p615-624, 2015.

[13] R.Davice,”The Internet of Things Opportunties and challeng”, European, p.p.1-8, 2015.

[14] G.Price, “The Internet of Things 2015”, State of THE Market: Internet of Things 2015, Verison wireless company p.p1-24, 2015.

[15] X.Xingmei, Zh. Jing,W.He, “Research on the Basic Characteristics, the Key Technologies, the Network Architecture and Security Problems of the Internet of Things”, 3rd International Conference on Computer Science and Network Technology (ICCSNT), Dalian, China, IEEE, p.p.825-828, 2013.

[16] Y.Challal, E. Natalizio, S.Sen, and A.Maria Vegni “Internet of Things security and privacy: Design methods and optimization”, Add Hoc Network, vol.32, Science Direct, p.p1-2, 2015.

[17] Ch. Qiang, G.Quan, B.Yu, L.Yang, “Research on Security Issues of the Internet of Things”, International Journal of Future Generation Communication and Networking (IJFGCN), vol.6, NO.6, IEEE, pp 1-10, 2013.

[18] Afsoon Yousefi , Seyed Mahdi Jameii “Improving the Security of Internet of Things using Encryption Algorithms”

[19] Tsvetko Tsvetkov Betreuer: Alexander Klein “RPL: IPv6 Routing Protocol for Low Power and Lossy Networks” Seminar SN SS2011, doi: 10.2313/NET-2011-07-1_09 Network Architectures and Services, July 2011

[20] Internet Assigned Numbers Authority (IANA). Internet Control Message Protocol version 6 (ICMPv6) Parameters. http://www.iana.org/assignments/, 2011.

[21]. Zadeh, L. Fuzzy sets. Inf. Control **1965**, 8, 338–353.

[22]. Samadzadeagan, F.; Saeedi, S. Fusion of Remotely Sensed Data in the Context of Sensors, Features and Decisions. WSEAS Trans. Environ. Dev. **2005**, 1, 363–371.

[23]. Saeedi, S.; El-Sheimy, N.; Malek, M.; Samani, N. An ontology based context modeling approach for mobile touring and navigation system. In Proceedings of the The 2010 Canadian Geomatics Conference and Symposium of Commission I, ISPRS Convergence

in Geomatics–Shaping Canada’s Competitive Landscape, Calgary, Canada, 15–18 June 2010.

[24]. Yang, J.; Lu, H.; Liu, Z.; Boda, P.P. Physical Activity Recognition with Mobile Phones: Challenges, Methods, and Applications. In Multimedia Interaction and Intelligent User Interface; Springer-Verlag: Berlin, Germany, 2010; pp. 185–213.

[25] Stankovic, JA , “Research Directions for the Internet of Things”, IEEE Internet of Things, vol. 16, no.2, May 2015.

[26] Lang Li, Botao Liu , Hui Wang, ” QTL: A new ultra-lightweight block cipher” in Elseiver, April 2016.

[27] Amendola, S, Lodato, R, Manzari, S, Occhiuzzi, C & Marrocco, G, “RFID Technology for IoT-Based Personal Healthcare in Smart Spaces”, IEEE Internet of Things, Vol. 03, no.04, March 2014.

[28] P. Nandhini1, Dr.V.Vanitha2 “A Study of Lightweight Cryptographic Algorithms for IoT” International Journal of Innovations & Advancement in Computer Science IJIACS ISSN 2347 – 8616 Volume 6, Issue 1 January 2017

[29] Liang Xiao_†, Xiaoyue Wan_, Xiaozhen Lu_,Yanyong Zhang‡, Di Wu§ “IoT Security Techniques Based on MachineLearning” arXiv:1801.06275v1 [cs.CR] 19 Jan 2018

[30] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, “Internet of Things: Security vulnerabilities and challenges,” in Proc. IEEE Symposium on Computers and Commun, pp. 180–187, Larnaca, Cyprus, Feb. 2015.

[31] R. Roman, J. Zhou, and J. Lopez, “On the features and challenges of security and privacy in distributed Internet of Things,” Computer Networks, vol. 57, no. 10, pp. 2266–2279, Jul. 2013.

[32] G. Han, L. Xiao, and H. V. Poor, “Two-dimensional anti-jamming communication based on deep reinforcement learning,” in IEEE Int’l Conf. Acoustics, Speech and Signal Processing, pp. 2087–2091, New Orleans, LA, Mar. 2017.

[33] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, “PHY-layer spoofing detection with reinforcement learning in wireless networks,” IEEE Trans. Vehicular Technology, vol. 65, no. 12, pp. 10037–10047, Dec. 2016.

[34] L. Xiao, Y. Li, X. Huang, and X. J. Du, “Cloud-based malware detection game for mobile devices with offloading,” IEEE Trans. Mobile Computing, vol. 16, no. 10, pp. 2742–2750, Oct. 2017.

[35] Z. Yan, P. Zhang, and A. V. Vasilakos, “A survey on trust management for Internet of Things,” Journal of Network and Computer Applications, vol. 42, no. 3, pp. 120–134, Jun. 2014.