Wireless control, distributed figuring, intrusion discovery, disaster management

Wireless sensor network is an accumulation ofhuge number of sensor nodes organized or dispersed that combine to form a gridwhich is used to sense information such as pressure, degree, sound, tremor, movement etc. after collecting data through sensor nodes the data iscollectively send to a sink node where statistics can be stored and figure out. The data which is required can be rectifying by asking queries and gatheringresult from the base station and the facts gathered by sensor nodes is in itsaccurate form. These devices are implanted at a cheaper cost than traditionalwired system.

All sensor nodes consist of a battery enabled chip, a radio Transreceiver, a memory chip and a position finding system 1. Sensor nodes areconstrained devices consist of less efficient battery backup, a small memorychip in relation to storage and other limited resources owing to the restrictedstructure of sensor nodes. The main issuewith the wireless sensor web is the nodes are abandoned for a long period oftime or forever, have a short duration of lifetime and the topology used forimplementation is generally unknown. The main challenges in WSN web emerge dueto restricted resources the nodes have and deployment of these nodes in adverseconditions, where it is almost insuperable or invincible for humans to attendor observe the sensor nodes Owing to the negligence it may effects theeffectiveness of many applications in the field of military or publicapplications such as safety, tactical surveillance, inventory control, distributed figuring, intrusion discovery, disaster management and detectionambient conditions. Many applicationsrequest the sensor nodes to be small in size and limit the transmission rangeto minimize the chances of detection. This results in additional constraints onother resources such as

speed, size of memory, RF bandwidth and lifetime ofsensor node. Therefore, efficient techniques of communication are essential forenhancing the time period of survival of a sensor node and increasing theamount of acquiring data and reducing the communication latency of suchwireless devices 2. In spite of having limited communication and computationcapabilities a WSN that contains of thousands or millions of sensor nodesenhances the different ways through which records can be placed from physicalenvironment with highly precise knowledge about the data that is to be sensed.

But when it comes to amalgamation of WSN with the existing Internet it comeswith several number of challenges. This dissertation discusses the challengesand the finest technique to interface wireless sensor network with the IoT tomonitor the environmental parameters is analyzed. 1. 1. MOTIVATIONWSN is a setup ofsensor nodes that convey statistics or data between nodes that are not wired orbind up by electrical conductors. Most of the wireless sensor communicationtechnology uses radio waves and micro waves in direction to transferinformation between the points which are known as nodes.

One anotherapplication field of wireless communication is WSN. WSN is a distributedsystem, containing resource or constrained nodes that work in an ad hoc mannerusing multi-hope communication 3. WSNs and Internet are integrated as a newapplication area called IoT, covering almost every area in current daily life4. IoT encourages several novel and existing applications such as environmentmonitoring, infrastructure management, public safety, health care andwell-being, home and office security, transportation, and military applications2. The complexity of a WSN 3, which interpret sensing

and ID activitiesinto services using WSN with WSN middleware and access networking. It can use:(i) different communication platforms such as Wi-Fi, wireless LAN, 3G and 4G.

(ii) different devices which are established on different processors such asvarious types of PDA, smart phones and laptops and (iii) all these platformsand devices being built on different architectures such as centralized, distributed or peer-to-peer. 1. 2. WIRELESS SENSOR NETWORK WSN is acollection of huge number of sensor nodes or that combine to form a networkwhich is used to sense data such as pressure, temperature, sound, tremor, motion etc. WSNis regard as a revolutionary information collecting methods, techniques to build the information & communication system which willgreatly improve the reliability & efficiency of infrastructure systems. Compared with the wired solution, WSNs feature easier deployment and betterflexibility of devices. Due to quick advancements in the technology and bloomin the field of sensor nodes, WSN will become the main technology for IoT.

A WSN basically structuresless; they are dispersed or unorganized nodes combine together to observe anarea over which they are implanted to get data about the conditions of the surroundings. Here we are defining dual types of WSNs called as structured WSN &unstructured WSN. Unorganized WSN has sensor nodes dispersed closely and aremostly implanted in ad-hoc network field, i. e. nodes are deployed randomly inthe aimed area.

In organized wireless sensor network sensor nodes are deployedin pre-determined locations. These sensor nodes are energy limited and

specificapplication oriented. Thus, the power management of sensor node is essentialfor effective network operations and particular sensor networks are determined bythe following two

parameters:

Figure 1. 1.

Wireless Sensor Network5 1. 2. 1.

Data flow patterns In sensornetworks, each node is an independent data collection device. Periodicallyapiece sensor node in the wireless network sends its readings to central workstation. Sometimes, the chief workstation will be interested in specific informationfrom nodes insuch case it inserts the query into the network and it is propagated. Thennodes with the data will reply to the query with the relevant information. 1. 2.

2. Energy constraints The sensor nodesin the networks are battery operated with limited recharge capabilities. Theprimary system enactment metric is the energy effectiveness of operation. 1. 3. INTEGRATING WIRELESS SENSORNETWORK AND INTERNET OF THINGS The integrationbetween the Internet and a WSN is classified into three.

They are (i) front end(ii) (ii) Gateway

and(iii) (iii) TCP/IP. A WSN is fullyindividualistic from the internet (i. e. front end), can only be in touch withinternet hosts and transfer data across it (i. e. gateway), or allow areconcilable network layer protocol (TCP/IP). Its firstresemblance is the Front-End solution. The solutions are the peripheralInternet hosts and the sensor nodes does not communicate directly with eachother.

In fact, the WSN is completely individualistic from the internet, so itcan deploy its self -benefitted group of protocols. All interactions among theexternal world and the sensor network will be managed by a centralized device, such as a base station as shown in Figure 1. 2. The sink nodecollects all the transmission throughout the nodes with a WSN, and the sinknode may also give permission to read or write on data gathered to additional outsideobjects through commonly used interfaces. In addition, any query coming fromthe Internet hosts will be always traversing the base station (B). WSN internet B Figure1.

2. Frontend solution for integrating IoT and WSN. The 2ndapproach is the Gateway solution, considers the presence of a device (e. g.

base station)it is used as anapplication layer gateway, having responsibility of interpreting the lowerlayer protocols among the networks (e. g. TCP/IP and proprietary) and routingthe information from one point to another, as shown in Figure 1. 3. Shows thatthe result, Internet hosts and sensor nodes can be capable to address eachother and exchange information without establishing a truly direct connection.

thisapproach, the WSN is still liberated from the Internet, and all queries stillneed to traverse a gateway device. However, sensor nodes can be capable toprovide web service interfaces to external entities while maintaining theirlower layer protocols. WSN internet G Figure1. 3. Gateway (G) solution for integrating IoTand WSN.

The 3rdapproach, the TCP/IP solutions approach, sensor nodes are

implementing the TCP/IP stack thus nodes can be considered asfull-fledged

elements of the Internet. Any host of the internet can connect directlywith them, and vice-versa. This is the most appropriate technique forimplementing full amalgamation of WSN and IoT. A significance of thismethodology is that sensor nodes are no longer able to use specific WSNprotocols. The Internetenabled nodes behave i) As a front-end, efficiently segregating the wireless sensor network sensors from the Internet, or ii) As gateways, allowing direct data exchange between sensors and the central system. There are numerousaspects that need to be taken care of before choosing a certain integrationapproach. The main factors are summarized in the succeeding paragraphs: 1.

Resilience. WSN directly provides its services toexternal entities are quite vulnerable against security attacks. Gateways andsensor nodes need to be capable to include security mechanisms that increasetheir robustness against attacks.

2. Securityof the communication channel. It is necessary to analyze how mechanisms such as TLS could becast-off to offer an end-to-end secure channel. In fact, it is likewisenecessary to study the different key exchange mechanisms that would be used. 3. Accountability. For an Internet-enabled WSN, it mightbe fascinating to advance a distributed system that is capable to record theinteractions with the users of the system. By store all communications, wecould be capable to recreate security incidents and abnormal situations.

4. Functionality. There might be some applications wherethe sensor nodes do not need to be aware of the Internet.

Example, WSN whosetasks are limited to collect information and answer to user queries notsupposed to contact any Internet service without permission. 5. Hardware. A specially controlled sensor node mightnot be capable to be directly connected to the Internet owing to the memoryrequirements of the different security mechanisms. 6. Inherentweaknesses. Internetempowered sensor devices are susceptible to countless more diverse types of securityattacks, ranging from DoS attacks to exploit attacks.

7. Networkredundancy. Among the several nodes, a sensor nodemight provide same ramification while increasing redundancy, but in TCP/IPnetwork an external node will ask for services to be provided by specific nodethrough their IP address. It results in development ofspecific mechanism in TCP/IP network to overcome from the exceptionalconditions (i. e. unreachable nodes).

8. Protocoloptimizations. Most wireless sensor network definite protocols embrace assuredmechanisms that permit a network to self-heal itself and to enhance itsinterior behaviour. After knowingabout the different integration approaches, it looks like TCP/IP is one of theefficient way to successfully integrate wireless sensor network with internet. In term of other solution approaches, like asa Front-End solution; the nodescan solitary access those services that are implemented in the central system(server). In fact, it is actually extra perplexing to guarantee the safety ofWSN that make practice of the TCP/IP solution. But for considering the environmentalmonitoring Front end solution is the simple, easy and effective way ofintegration.

For measuring the environmental parameters, the information willbe minimized by the base station. The data which is necessary to monitor onlydirect to the Internet. 1.

5. SECURITYThere had beenmany Hollywood films on how the upcoming will look – and the IoT vision comesclose to the Hollywood vision. There is single common theme across bothvisions: machines become very powerful as a whole within a highly automatedsociety. The question of individual privacy and security within this for theindividual becomes additional problematic as the complex chain within which thesecurity has been created is countless and among the links which is weakestthat defines the summary of safekeeping of the network. We are provided withIPv6 through which we are capable to connect to billions of data points throughIP addresses that will result in a new world – query is will they can all besecured to a level that can ensure individual privacy rights and secure thesystems from malicious attacks. In traditional TCP/IP networks, security isbuilt to protect the confidentiality, integrity and availability of networkdata.

It makes the system reliable and protects the system from maliciousattacks which can lead to malfunctioning systems and information disclosure. Asthe characteristic of node and application, WSN security is a not only needstraditional security protection, but also need the special requirements oftrust, security and privacy (TSP) WSNs 4. Roughly, thesecurity threats can be categorized as: physical (local) attacks andnon-physical (remote) attacks. Physical attacks are executed by attackers whichforce their way into the physically unprotected thing and effort to negotiationit in different ways 6,

7. 1. 5. 1. Trust, security and privacy management (TSP)Trust, securityand

privacy in wireless sensor network, completely be determined by theapplication environment, the protection needed for integrity, availability, confidentiality, non-repudiation, and user privacy.

It supports systemintegrity, reliability by protecting the system from malicious attacks. WSNrequires the nodes to be protected against tampering of nodes, protect thetransmission medium and routing in the network layer 3. TSP logging/ auditfunctions may be required to detect attacks. The Trust, security and privacy issues in WSN includes authentication of sensor nodes, encryption of exchanged data, access control etc.

The TSP requirements of WSNincludes node security, key management, crypto algorithms, secure routing, anddata aggregation 6. Types of privacythreats: 1. 5. 1. 1. Confidentiality Confidentialitydescribes the avoidance of revelation of data to unauthorized entities.

We wantto achieve confidentiality to prohibit privacy threat and eavesdroppingattacks. Please note that an invader can observe communication patterns of auser even if confidentiality is provided by the connection, allowing him toinfer private information about the user anyway. This attack is justcomplicated when confidentiality is provided, but not fully averted. 1.

5. 1. 2. AuthenticityAuthenticityguarantees that all parties involved in the communication are who they claimthey are. 1. 5. 1. 3.

IntegrityIntegrity isviolated if a message can actively be altered during transmission without actualityspotted. If message integrity and authenticity

is guaranteed, man-in-the middleattacks can be averted. 1. 5. 1. 4. Availability Ensuring thesurvivability of services to parties when needed, even during a DoS attack. 1.

5. 1. 5. Authorization Access to theresources by an authentic entity. 1. 5.

1. 6. Data Freshness It makes sure thatno unauthorized node can replay old messages. Similarly recognized as keyfreshness. All abovementioned services can be attained by means of some of the cryptographicmechanisms such as block ciphers, signature algorithms and hash functions andsome non-cryptographic mechanisms, those leads to authorization and othermentioned security policies implementation aspects. In constrained environments such as IoT: So far, the listedsafety fears and goals can be applied to arbitrary networks. We, however, are focusingon constrained networks, therefore we need to appearance at the additional consequencesthat arise in constrained environments.

One additional problem is the minorpacket size, which may result in fragmentation of larger packets in securityprotocols (e. g., a large key exchange message). This may open new attackvectors for state enervation DoS attacks 7. Further, the size and numeral ofmessages should be minimized to reduce memory requirements and optimizebandwidth usage, while maintaining high security standards.

When reducing orsimplifying a security protocol in direction to minimize energy consumption, one must also expect losses in the security quality 8. An appropriatetrade-off must be found for apiece distinct environment. Another problem is thestill existing gap between Internet protocols and the

IoT, namely 6LoWPAN andCoAP, due to performance reasons. The differences mentioned can be filled usingprotocol interpreters at gateways, but that can lead to major disadvantage ifend-to-end security methods amongst internet host and IoT devices are implanted. When a message is protected by means of message authentication codes orencryption or both, the protected fragments of the message become immutable. Thus, making rewriting not possible for the translators 7. Figure 1. 4 TSP architecture for WSN's 1.

6. INTERNET OF THINGS The initial ideaof IoT was proposed by MIT Auto-ID Labs at the end of 1990'swhich originatedfrom the requirement of logistics. ITU Internet Reports 20059 indicatedthat we are in the direction of an omnipresent network civilization, one inwhich networks and networked devices are everywhere. The notion of " Things" ininternet of things has been generalized to ordinary objects at present, and theinterconnection technology is also extended to all networking technologies, including RFID (Radio Frequency Identification). 1. 6. 1.

Three importantcharacteristics of IoT. Ordinary objects are instrumented. Define as the customary objects such as chair, food, clothes etc. can be addressed individually using RFID chip, bar code and many more like that. Autonomic terminals are interconnected. It states that the instrumented physical entities are associated as autonomic web Pervasive services are intelligent. A widely interrelated network, hire each object participates in the service stream to mark the pervasive service intelligent. For example, the sensor nodes of automobile transport network or human transport

network be able to observe the status of lane or the body of driver to acquire real-time information for guiding driving.

Therefore, Internet of things is a refined wide-ranginginter disciplinary technology, e. g., surrounding multiple ranges such ascomputer science, infrastructures, microelectronics and sensor technology.

IoTis closely-related to the Internet, mobile communication networks and WSN. Comparinginternet of things with WSNs, Internet, omnipresent systems and additionalexploration. 1. 6. 2. Purposesof IoTCompared with the traditional information net- works, threenew goals of IoT, i. e., more widespread interconnection, extra concentrated statisticsinsight, and additional wide-rangingintellectual services.

IoT ranges the interconnectionamongst the information equipment’s, such as system and mobile phone, to theinterconnection of all intelligent or non-intelligent physical objects. It hasthe succeeding outstanding characteristics: Richness in the quantity of devices. The quantity of the associated devices will abruptlyincrease from some billions to over hundreds of billions, containing a multitude of equipment’s, sensors, actuators, means of transportation, and devices committed with. Comprehensiveness in the kind of networking devices (networking components) might be powered by the electric power directly or by batteries; the computation and communiquécapabilitymight be momentouslyunlike, e. g., more or less devices even might not have at all computational capability.

Extensiveness in the connection. The devices might be associated in a wired or wireless approach; the communication could be a single hop or multiple

hops; the connection can be strong state routing or statistical weak state routing. Thus, in such a hefty scale heterogeneous network, we essentiallyencounter the challenges of extremely resourceful interconnection of networkentities. 1. 7.

OBJECTIVE OF THE THESISWhen this methodwas proposed few goals were set, as follows 1. To Analysis ofSecurity Methods and some cryptography algorithm. 2. To study ofNetwork Simulator NS-23.

To study aboutECSM techniques before implementation in network simulator. 4. Implement ECSMtechniques in NS-2. 35. 5. Compare theExisting security and proposed security approach in WSN.

6. Compute theresult Delay, PDR, Energy, Throughput. 1. 8. ORGANIZATION OF THE THESISInthis chapter we discussed about WSN, IoT, Security level, Objectives of IoT.

Chapter 2discusses about the literature survey i. e. the work that has already been donein this field. Chapter 3consistof the tool overview that has been used for implementing the proposed work. Chapter 4 discusesECSM (proposed work) and implementation. Chapter 5 includesthe result ad analysis phase, I this we compare the results of the base paperwith the implemented technology.