International Journal of Innovative Research in Information Security (IJIRIS) ISSN: 2349-7017(O)
Issue 2, Volume 3 (March 2015) ISSN: 2349-7009(P)
www.ijiris.com

Authentic Data Exchange in Wireless Sensor Networks Ensuring Integrity and Confidentiality

[1] Surya.M
PG Student
KCG College of Technology
Chennai

[2] N.Nityanandam
Professor
KCG College of Technology
Chennai

Abstract: ***This task is expected to give Authentication, respectability and secrecy in remote sensor systems (WSNs). Information trade between sensor hubs and the CHN is encoded utilizing symmetric key encryption framework. CHN gathers the entire message from sensor hubs and by utilizing accumulation calculation, it totals the messages. The information trade between the CHN and Sink is encoded utilizing open key encryption framework for validness and privacy. If there should arise an occurrence of static hubs in remote sensor organizes, the CHN which has totaled the encoded message from source hubs encodes the amassed message utilizing its own particular private key to demonstrate realness and again scrambles utilizing open key of the sink to guarantee privacy and sends it to the sink. The Sink on getting the message from CHN unscrambles the message utilizing its own particular private key and the again decodes utilizing open key of CHN. If there should arise an occurrence of portable hubs in remote sensor organizes, the CHN is chosen in view of the lingering vitality as essential parameter utilizing the R-HEED calculation (Rotated Hybrid Energy Efficient Distributed Clustering). At that point the CHN does likewise handle as on account of static hubs. It guarantees that the message is not modified or adjusted by the assailant. It additionally guarantees that the aggressor can't get the information from CHN to sink and the information is genuine. Confirmation is given by the private key and Confidentiality is given by general society key.***

Keywords: ***Wireless sensor network, Ad hoc, mutual authentication, Key agreement, Smart card, Internet of Things***

I INTRODUCTION

We are evermore encompassed by pervasive, canny interconnected items which captivate us with new practical viewpoints on our ordinary lives, like RFID, cell phones, semantic web, remote sensors, and so on. This can be seen as the Internet of Things (IOT) thought, which was declared 10 years prior. The thought was that later on everything would be open, sensed, and interconnected inside the worldwide, dynamic, living structure of the Internet. Remote sensor systems (WSN) assume a critical part with respect to this idea, since they cover a wide application field by gathering different natural data. In the early years WSNs began as straightforward and undecided exploration extends essentially persuaded and financed by the military, DARPA (Defense Advanced Research Projects Org) [2]. These early military-financed WSN research tasks, as indicated by their sort of uses, exhibited a meaning of the WSN as a substantial scale, remote, specially appointed, multi-jump, un-apportioned system of homogeneous, small, generally stable sensor hubs which are haphazardly conveyed inside a specific range of investment. Such a definition does not make a difference to the greater part of today's WSN applications, since WSN applications can likewise be heterogeneous, single-bounce, foundation based, have portable sensor hubs, and so on. Around then the WSN research papers concentrated just on the hypothetical and wide practical employments of WSNs, at the same time the exploration and practical utilization of WSN has fundamentally expanded throughout the most recent few years. Today we talk about the utilization of WSN for activity checking, pipeline checking, avalanche identification, methane spill recognition, outskirt watch, accuracy farming, restoration applications, research center mentoring, resource following, continuous soccer playing checking and numerous more. A rundown of genuine useful WSN undertakings was summed up by Romer and Mattern. Initially it was believed that WSN would just be homogeneous, comprising just of equivalent sensor hubs.

Today we additionally talk of heterogeneous WSNs since sensor systems can be manufactured with distinctive sorts of hubs, some all the more computationally-capable than others. In perspective of the IOT idea, the heterogeneity of a WSN is not by any means the only thing quickly adjusting, henceforth the foundation has moved from principally infrastructure based systems, where hubs can just impart straightforwardly with the base station, to specially appointed systems whereby hubs can likewise correspond straightforwardly with one another and with rest of the world. WSNs are getting to be evermore various and interconnected with the IOT, along these lines showing new open doors anyhow likewise challenges which need to be tended to. An illustration of such would be a remote client who needs to get to a specific sensor hub of the WSN. Such a client needs to be approved and, if done decidedly, permitted to accumulate information from or send charges to the sensor hub. Since the most imperative and unique normal for WSNs is their asset obliged construction modeling, a lightweight security arrangement is obliged, along these lines urging the security outline to be more judicious. A key test is the way to empower the foundation of a imparted cryptographic key in a safe and lightweight way, between the sensor hub and the client outside the system.

© 2014-15, IJIRIS- All Rights Reserved

Common validation is additionally required for such a situation, and is exceedingly vital since everything gatherings need to make certain of the authenticities of every last one of elements included. Various cryptographic plans for the security of the WSN have been proposed however not very many have tended to the previously stated situations, difficulties, and prerequisites. This was the inspiration for us to create also propose a test particular cryptographic plan, which utilizes an uncommon four-stage verification show that we accept is the most proper for the specified situation, at the point when a remote client needs to interface with a sensor hub inside a WSN. Since our plan uses shrewd cards for clients to verify, the security building design is likewise savvy card arranged. This paper is proposed to give Authentication, Confidentiality and Integrity for information trade in remote sensor systems (WSNs). Remote Sensor Networks comprising of hubs with constrained force are sent to assemble helpful data from the field. In WSNs it is basic to gather the data in a secured and effective way. In the venture, to guarantee genuineness, classifiedness and uprightness between the source and sink, both symmetric key encryption and open key encryption frameworks are utilized.

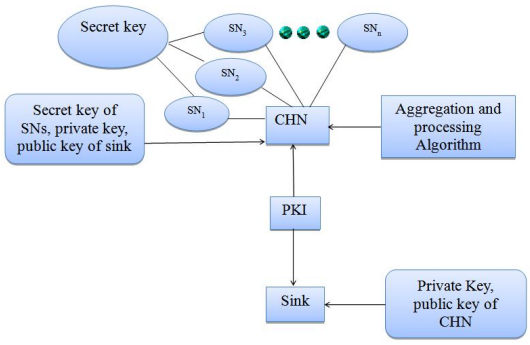

Fig.1 System Architecture

If there should be an occurrence of static hubs in remote sensor arranges, the groups are shaped in which there are N source hubs in a bunch to exchange the message to the Sink. Every source hubs are given mystery key for symmetric key encryption. A middle of the road hub known as Cluster Head Node (CHN) which is more compelling than the source hubs go about as a preparing hub to total the messages got and safely send the same to the sink. The Cluster Header Node (CHN) which is the moderate hub between the source and sink gets the encoded message, forms it and totals the message for giving confirmation and privacy. There are N source hubs inside the closeness of the CHN. The CHN will have its ID, shared (with source hubs) mystery keys, its own particular private key and open key of sink for encryption and decoding procedure.

The CHN gets the scrambled message from all the source hubs inside group and decodes the message utilizing the imparted mystery key of all source hubs. It then totals the messages. Total and handling calculation in CHN is utilized to perform the errand of collecting the encoded message from the source hubs. Hence information trade between sensor hubs and the CHN is encoded utilizing symmetric key encryption framework for secrecy. After arranged collection in CHN, it does the procedure of sending the genuine message to the Sink by open key foundation. The Sink has its own private key and open key of CHN. The CHN which has collected the message from source hubs scrambles the totaled message utilizing its own private key to demonstrate validness and again encodes utilizing open key of the sink to guarantee privacy and sends it to the sink. The Sink on accepting the message from CHN unscrambles the message utilizing its own private key and the again decodes utilizing open key of CHN.

If there should be an occurrence of portable hubs in remote sensor organizes, the groups are framed in which there are N source hubs inside group to exchange the message to the Sink. Every source hubs are given mystery key for symmetric key encryption. The CHN is chosen taking into account the remaining vitality as essential parameter utilizing the R-HEED calculation (Rotated Hybrid Energy Efficient Distributed Clustering). At that point the CHN gets the encoded message from all the source hubs inside group and decryptes the message utilizing the mystery key of all source hubs, forms it and totals the messages. At long last the CHN which has totaled the message from source hubs scrambles the amassed message utilizing its own private key to demonstrate realness and again encodes utilizing open key of the sink to guarantee classifiedness and sends it to the sink. The Sink on accepting the message from CHN decodes the message utilizing its own private key and the again unscrambles utilizing open key of CHN.

II **RELATED WORK**

In this article [1] A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion, authors Muhamed Turkanovic, Bostjan Brumen and Marko Holbl, discuss about the Novel client verification and key understanding plan for heterogeneous impromptu remote sensor systems which empowers a remote client to safely arrange a session key with a general sensor hub, utilizing a lightweight

© 2014-15, IJIRIS- All Rights Reserved

key assention convention. This plan guarantees common validation between the client, sensor hub, and the portal hub (GWN), despite the fact that the GWN is never reached by the client. This plan has been adjusted to the asset compelled structural engineering of the WSN, accordingly it guarantees generally fixed sensor hubs are arbitrarily conveyed inside a specific zone of investment. In this article authors [2] Oscar Delgado-Mohatar, Amparo Fuster-Sabater, Jose M. Sierra discuss about the A light-weight verification model for remote sensor systems made out of a key administration and a validation convention is exhibited. It is in light of the utilization of basic symmetric cryptographic primitives with low computational prerequisites and it can lessen vitality utilization. It likewise scales well with the extent of the system, because of it just obliging one traded message, autonomously of the aggregate number of hubs in the system. In this article authors [3] Claude Castelluccia, Einar Mykletun, Gene Tsudik, discuss about "Efficient Aggregation of encrypted data in Wireless Sensor Networks"**.** Total gets to be particularly difficult if end-to-end security in the middle of sensors and the sink is needed. A straightforward and provably secure additively homomorphic stream figure that permits productive accumulation of scrambled information. In this article authors [4] Merad Boudia Omar Rafik and Feham Mohamed, discuss about the "RSAED: Robust and Secure Aggregation of Encrypted Data in wireless sensor networks". It introduces RSAED that permits respectability confirmation at halfway hubs, guarantees the base station to get ciphertexts which come just from genuine hubs furthermore enhances the effectiveness. In this article authors [5] Sumit Chaudhary, Neha Singh, Avinav Pathak and A.K Vatsa, discuss about the "Energy Efficient Techniques for Data aggregation and collection in WSN". The productive and viable structural engineering and instrument of vitality proficient procedures for information accumulation and gathering in WSN utilizing standards like worldwide weight estimation of hubs, information accumulation for bunch head and information conglomeration systems utilizing information 3D shape total. In this article authors [6] Wail Mardini, Muneer Bani Yassein, Yaser Khamayseh, Barraq A.Ghaleb, discuss about the "Rotated Hybrid, Energy-Efficient and Distributed (R-HEED) Clustering Protocol in WSN", IEEE transactions on communication, volume 13, 2014. Crossover, Energy-Efficient, and Distributed bunching methodology (HEED) is viewed as a standout amongst the most vitality productive grouping calculations that uses intra-correspondence expense and lingering vitality to choose the Cluster Heads (CHs) by analyzing diverse between bunch steering conventions over HEED and assess their execution. Also, an improved rendition to HEED, specifically Rotated HEED (RHEED), is proposed. The altered form leads the setup stage as per certain principles and calendar, with HEED performs this venture toward the start of a few rounds. Toward the start of each round the CHs hold up a predefined time of time to get a re-bunching message from the BS. On the off chance that they don't get the re-bunching message, they will keep pivoting the group head inside the same bunch.

III **SYSTEM OPERATION**

A remote sensor hub is a mainstream arrangement when it is troublesome or difficult to run a mains supply to the sensor hub. The remote sensor hub is regularly set in a hard-to-achieve area, changing the battery consistently can be unreasonable and badly designed. A vital viewpoint in the improvement of a remote sensor hub is guaranteeing that there is constantly satisfactory vitality accessible to power the framework. In these cases, reaping neighborhood vitality to power the remote sensor hub is attractive in [7]. There are diverse sorts of vitality that can be reaped in fig 3.1, the most well-known source is sunlight based. A sun powered controlled remote sensor hub arrangement gathers and aggregates vitality over a developed time of time and uses a low-spillage, high-limit vitality holder, for example, a dainty film battery. This class of vitality gathering framework is the most adaptable and normally consumes control in short blasts of high-power utilization. These remote sensor hub frameworks invest a dominant part of the time in a low-power rest mode, are constantly fueled and harvest vitality at all times, making them perfect for in modern controls, building security, keen home and security mechanization and in agrarian frameworks. The area is made arrangements for sensors and sinks. It portrays what number of sensors are to be found. It is utilized to depict where the sensors are observed.

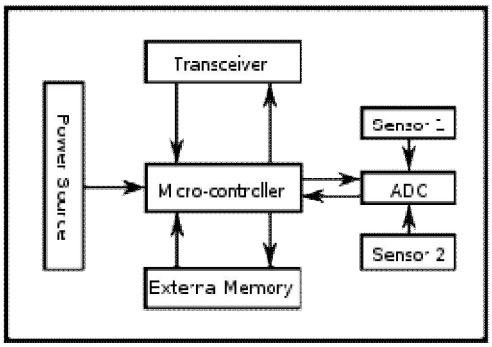

Fig. 3.1 Location plan

Entomb hierarchical systems develop as a consequence of the interdependencies between associations that guarantee associations to collaborate with one another and lead in time to system structures.

© 2014-15, IJIRIS- All Rights Reserved

Where progressive plans can be deliberately arranged, systems are reactionary since they develop out of context oriented occasions that start the arrangement of a communitarian system. Despite the fact that system development is decently concentrated on, the methodology in which systems start to exist and develop through time is not also known. Mostly because of the troubles regarding information gathering and investigation. This is particularly the case for open area systems since system development studies are overwhelmingly centered around the private part expressed that helpful between hierarchical relations experience three dreary stages: 1) arrangement stage in which associations arrange about joint activity 2) a pledge stage in which associations achieve an understanding and focus on future activity in the relationship and 3) an execution stage where joint activity is really performed. These three stages cover and are redundant all through the between authoritative relationship. The Node is instated to begin the procedure. The id, mystery key, areas are instated before sending the sensor hubs which are all normal to both CHN and source hubs. Node hub sending is an essential issue to be understood in Wireless Sensor Networks (WSNs). A fitting hub arrangement plan can lessen the multifaceted nature of issues in WSNs as, for instance, directing, information combination, correspondence, and so forth. Besides, it can expand the lifetime of WSNs by minimizing vitality utilization.

The hub is conveyed to indicate the aggregate life period. Hub is conveyed taking into account area and time of introduction. If there should arise an occurrence of static hubs in remote sensor organizes, the Cluster Header Node(CHN) which is a moderate hub between the source and sink gets the scrambled message from all the source hubs in every bunch and decodes the message utilizing the mystery key of all source hubs. It then totals the message of all the decoded message. The CHN which has totaled the scrambled message from source hubs scrambles the accumulated message utilizing its own particular private key to demonstrate credibility and again encodes utilizing open key of the sink to guarantee privacy and sends it to the sink. The Sink on accepting the message from CHN unscrambles the message utilizing its own particular private key and the again decodes utilizing open key of CHN.

Cluster development in this system for the gathering of group select then bunch head for the bunch and information transmission will happen after that group will get the relating messages for the youngsters hub The source hubs around the CHN are gathered to structure as groups. After bunch development, information transmission happens. In the event of portable hubs in remote sensor networks [8], the CHN is chosen taking into account the remaining vitality as essential parameter utilizing the R-HEED calculation (Rotated Hybrid Energy Efficient Distributed Clustering). At that point the CHN does likewise transform as on account of static hubs. Subsequently Authentication is guaranteed by scrambling the message utilizing its own particular private key and Confidentiality is guaranteed by encoding the message utilizing people in general key. Data transmission between group header hub and source hubs. After group arrangement send the information source hub to bunch head hub it will store the information [8]. There are N source hubs inside the nearness of the CHN. The CHN has N number of mystery keys. The sensor source hub scrambles the information with the mystery key. Information trade between sensor hubs and the CHN are encoded utilizing symmetric key encryption framework for classifiedness and message confirmation.

The Cluster head hub (CHN) is the sensor (source) hubs aggregator. CHN gathers the whole message from sensor hubs and by utilizing total calculation. It totals the messages from the source hubs [3]. The CHN gets the scrambled [5] message from all the source hubs inside group and decodes the message utilizing the imparted mystery key of all source hubs. It then totals the messages. Accumulation and transforming calculation in CHN [10], is utilized to perform the undertaking of accumulating the encoded message from the source hubs. Accordingly information trade between sensor hubs and the CHN is encoded utilizing symmetric key encryption framework for secrecy. After arranged total in CHN, it does the procedure of sending the genuine message to the Sink by open key framework. The Sink has its own private key and open key of CHN. The CHN which has amassed the message from source hubs encodes the accumulated message utilizing its own private key to demonstrate genuineness and again scrambles utilizing open key of the sink to guarantee privacy and sends it to the sink. The Sink on accepting the message from CHN unscrambles the message utilizing its own private key and the again decodes utilizing open key of CHN. PKI in the middle of CHN and sink PKI is that twofold encryption happens. To start with sink's open key with information is encoded which is again scrambled utilizing private key of CHN lastly the message is send to sink. The sink first decodes the message by open key of CHN which is again decoded by its own private key. The message got is not changed or modified. The got message is real. The CHN which has amassed the message from source hubs encodes the accumulated message utilizing its own private key to demonstrate genuineness and again scrambles utilizing open key of the sink to guarantee privacy and sends it to the sink. The Sink on accepting the message from CHN unscrambles the message utilizing its own private key and the again decodes utilizing open key of CHN. Data secrecy and verification. Information transmission in secret way in the encryption does the general population key encryption and confirmation assurance is guaranteed. The information trade between the CHN and Sink is encoded utilizing open key encryption framework for credibility and classifiedness. Privacy guarantees that the insurance of information from unapproved revelation. Therefore it guarantees that the message is not adjusted or altered by the aggressor. It likewise guarantees that the assailant can't get the information from source to sink.

© 2014-15, IJIRIS- All Rights Reserved

IV **RESULT & ANALYSIS**

As a result of simulation n network simulator-2, location planning, node deployment and node initialization are done in module 1 and cluster formation and data transmission between the Cluster Header Node and the sensor nodes are done in module 2. The cluster is formed and the data transmission between the CHN and source nodes is simulated in figure 4.1. In case of static nodes in wireless sensor networks, the Cluster Header Node (CHN) which is an intermediate node between the source and sink gets the encrypted message from all the source nodes in each cluster and decrypts the message using the secret key of all source nodes. It then aggregates the message of the entire decrypted message. The Node is deployed, initialized and clusters are formed. The source nodes communicate with the CHN to ensure the authenticity. The CHN collects the encrypted message from the source nodes and checks whether the message is authentic or not is shown in figure 6.2.

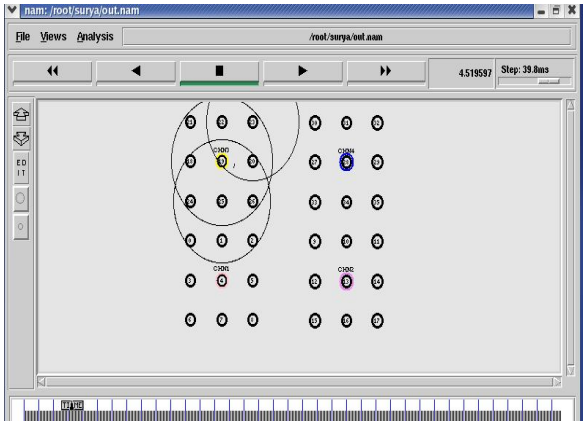

Fig 4.1 CHN in each cluster

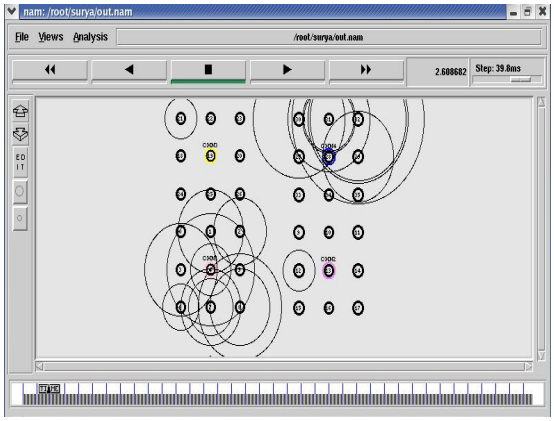

Fig 4.2 Data transmission

Thus the data exchange occurs between the CHN and the source nodes in which each cluster has its CHN. Each CHN is indicated in different colours. The CHN gets the encrypted message from the source nodes and decrypts the message using the secret key to perform the aggregation process. In figure 6.3, data transmission takes place between the CHN and other sensor nodes in the cluster to collect the information for checking the authenticity of the message in the source nodes. If the malicious nodes sends any corrupted message to the CHN, it will accept and check the message. The CHN after checking the message of malicious nodes from the attackers, the nodes are indicated as red colour in each cluster for ensuring the authentication and confidentiality. Thus the malicious nodes are identified in different colour to ensure the integrity as shown in figure 4.3. The CHN after checking the message of malicious nodes from the attackers, the nodes are indicated as red colour in each cluster for ensuring the authentication and confidentiality. Thus the malicious nodes are identified in different colour to ensure the integrity as shown in figure 4.4.

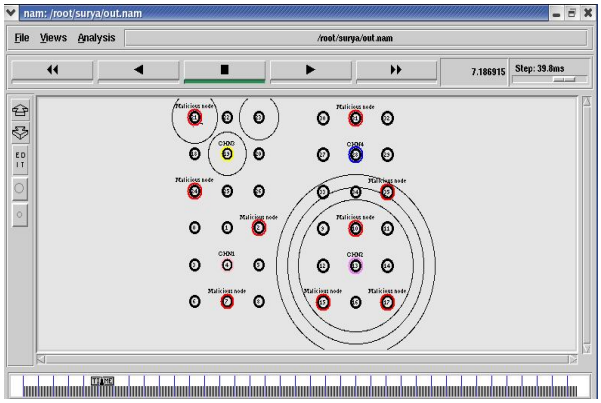

Fig 4.3 Checking the Authenticity

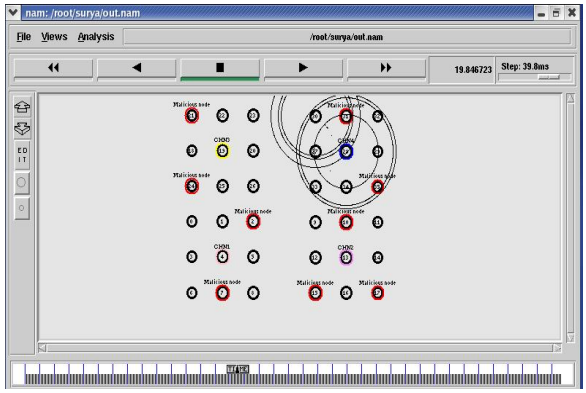

Fig 4.4 Malicious nodes identification

Authentication is the process of ensuring that the source is authentic and Confidentiality is the process of protecting the message from unauthorized disclosure. Integrity is the assurance that the message received are exactly as sent by an authorized entity.

© 2014-15, IJIRIS- All Rights Reserved

V CONCLUSION

Message privacy, respectability and verification are given while communicating something specific from source to sink. If there should arise an occurrence of static hubs in remote sensor organizes, the Cluster Header Node (CHN) which is a middle hub between the source and sink gets the encoded message from all the source hubs in every group and decodes the message utilizing the mystery key of all source hubs. It then totals the message of the whole decoded message. The CHN which has amassed the encoded message from source hubs encodes the accumulated message utilizing its own particular private key to demonstrate legitimacy and again scrambles utilizing open key of the sink to guarantee privacy and sends it to the sink. The Sink on accepting the message from CHN decodes the message utilizing its own particular private key and the again unscrambles utilizing open key of CHN. If there should arise an occurrence of portable hubs in remote sensor organizes, the CHN is chosen in view of the remaining vitality as essential parameter utilizing the R-HEED calculation (Rotated Hybrid Energy Efficient Distributed Clustering). At that point the CHN does likewise transform as on account of static hubs. Along these lines Authentication is guaranteed by encoding the message utilizing its own private key and Confidentiality is guaranteed by scrambling the message utilizing general society key. In this manner it guarantees that the message is not changed or altered by the aggressor. It additionally guarantees that the aggressor can't get the information from source to sink

.

REFERENCES

[1] Muhamed Turkanovic, Bostjan Brumen and Marko Holbl, “A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion”, Ad Hoc Networks 20 (2014) 96–112.
[2] Oscar Delgado-Mohatar, Amparo Fuster-Sabater, Jose M. Sierra, “A light-weight authentication scheme for wireless sensor networks”, Ad Hoc Networks (2011) 727–735.
[3] Claude Castelluccia, Einar Mykletun, Gene Tsudik, “Efficient Aggregation of encrypted data in Wireless Sensor Networks”, IEEE journal of networks, vol.5, 2005.
[4] Merad Boudia Omar Rafik and Feham Mohamed, “RSAED: Robust and Secure Aggregation of Encrypted Data in wireless sensor networks”, International Journal of Network Security & Its Applications (IJNSA), Vol.4-No.6, November 2012.
[5] Sumit Chaudhary, Neha Singh, Avinav Pathak and A.K Vatsa, “Energy Efficient Techniques for Data aggregation and collection in WSN”, International Journal of Computer Science, Engineering and Applications (IJCSEA), Vol.2-No.4, August 2012.
[6] Wail Mardini, Muneer Bani Yassein, Yaser Khamayseh, Barraq A.Ghaleb, discuss about the “Rotated Hybrid, Energy-Efficient and Distributed (R-HEED) Clustering Protocol in WSN”, IEEE transactions on communication, volume 13, 2014.
[7] Jong-Shin Chen, Zeng-Wei Hong, Neng-Chung Wang, San-Heui Jhuang, “Efficient Cluster Head Selection Methods for Wireless Sensor Networks”, IEEE journal of networks, vol.5-no.8, August 2010.
[8] Wail Mardini, Muneer Bani Yassein, Yaser Khamayseh, Barraq A.Ghaleb, ”Rotated Hybrid, Energy-Efficient and Distributed (R-HEED) Clustering Protocol in WSN”, IEEE transactions on communication, Volume 13, 2014.
[9] Atta ur Rehman Khan, Sajjad A.Madani, Khizar Hayat and Samee Ullah Khan, “Clustering-based power-controlled routing for mobile wireless sensor networks”, International journal of communication systems, vol-10, 2011.
[10] Nandini S.Patil, Prof. P.R.Patil, “Data Aggregation in Wireless Sensor Network”, IEEE International Conference on Computational Intelligence and Computing Research, Vol.4, 2010.

© 2014-15, IJIRIS- All Rights Reserved