iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** IX **Month of publication:** September 2016

DOI: http://doi.org/10.22214/ijraset.2016.9001

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Review of Wireless Sensors for Secure Routing

Prabhat[1], Garima Garg[2]
[1]M.Tech (CSE), [2]Assistant Professor
[1,2] Computer Science and Engineering Department, SGI, Samalkha,Panipat,India

Abstract- Sensor nodes may constitute the network for monitoring physical phenomena. Such network is called Wireless Sensor Network (WSN). Majority of WSN applications require at least some level of security. In order to achieve the needed level, secure and robust routing is necessary. Secure data transmission is a critical issue for wireless sensor networks (WSNs). In a cluster-based WSN (CWSN), every cluster has a leader sensor node, regarded as cluster head (CH). A CH aggregates the data collected by the leaf nodes (non-CH sensor nodes) in its cluster, and sends the aggregation to the base station (BS). In this paper, we have surveyed various security issues and their countermeasure to reduce these issues.

Keywords: Secure WSN, Energy Efficient WSN, Hierarchical routing, cluster head

I. INTRODUCTION

A. *Wireless Sensor Network*

A sensor network is composed of tens to thousands of sensor nodes which are distributed in a wide area. These nodes form a network by communicating with each other either directly or through other nodes as shown in figure 1. One or more nodes among them will serve as sink(s) that are capable of communicating with the user either directly or through the existing wired networks.

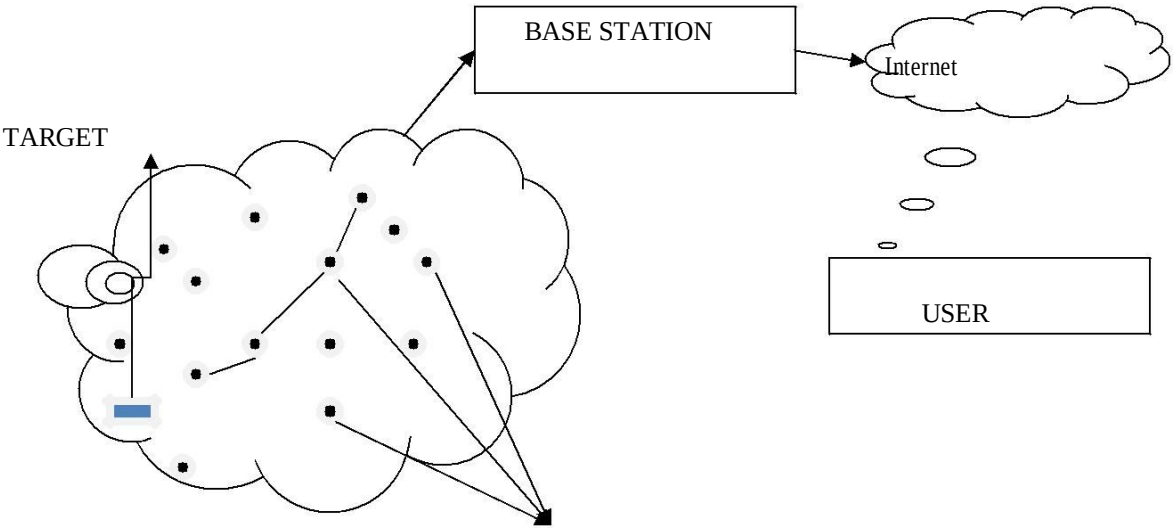


Fig. 1: Wireless Sensor Network architecture

B. *Traffic Patterns in WSNs*

In difference to traditional networks, the WSNs exhibit unique asymmetric traffic patterns. This is mainly faced due to the function of the WSN which is to collect data, sensor nodes persistently send their data to the base station, while the base station only occasionally sends control messages to the sensor nodes. Moreover, the different applications can cause a wide range of traffic patterns. The traffic of WSNs can be either singlehop or multi-hop. The multi-hop traffic patterns can be further divided, depending on the number of send and receive nodes, or whether the network supports in-network processing, into the following (figure 2):

Local Communication. It is used to broadcast the status of a node to its neighbors. Also it is used to transmit the data between the two nodes directly.

Point-to-Point Routing. It is used to send a data packet from an arbitrary node to another arbitrary node. It is commonly used in a wireless LAN environment.

Convergence. The data packets of multiple nodes are routed to a single base node. It is commonly used for data collection in WSNs.
Aggregation. The data packets can be processed in the relaying nodes and the aggregate value is routed to the base node rather than the raw data.
Divergence. It is used to send a command from the base node to other sensor nodes. It is interesting to investigate the traffic patterns in WSNs along with the mobility of the nodes, as node mobility has been utilized in a few WSN applications such as healthcare monitoring. One of the first attempts on doing this is provided in [2]. However, there is still an ongoing research area that will gather great attention on the following years.

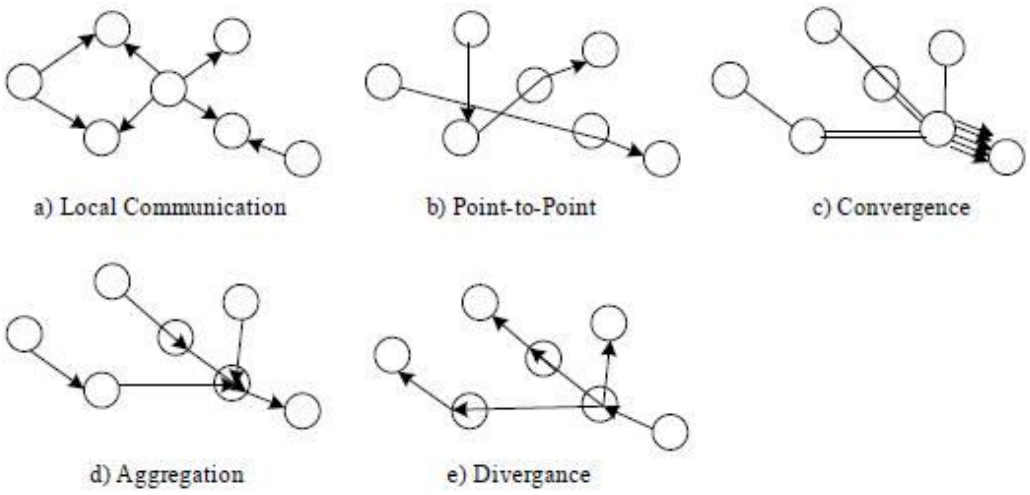


Fig. 2. The traffic patterns in WSNs

II. SECURITY ISSUES IN WIRELESS SENSOR NETWORK

Although, security concerns in mobile traditional networks apply to sensor networks, the solutions are not the same. Sensor nodes are tightly constrained in terms of energy, processing, and storage capacities. Once deployed, it is often very difficult to change or recharge batteries for such nodes. This constraint limits the number of conventional techniques that can efficiently be adopted to sensor networks. *Second,* wireless communication makes information more vulnerable to attacks. *Third,* WSN have to scale to larger numbers of entities than the current ad hoc networks. This requires careful handling of network size adjustments, which can happen by outside attack rather than internal deficiency or upgrade. An intruder might insert new foreign nodes to the networks that feeds false data or prevents the passage of true data. Node might be disabled by physical damage. *Forth,* sensor nodes placed into the physical environments; therefore it is often easy to compromise by an attacker. In addition, it is effortless to capture them physically and ruin them. *Fifth,* sensors networks composed of heterogeneous nodes with different capabilities. Identifying the possible threats that may face sensor networks will help in designing secure routing protocol Table 1 summarize the possible threats that may face routing protocol in sensor networks [1,6].

C. Black Hole Attack

In Black Hole attack [8] the attacker tries to collect most of the data of the network and later drops it. In our simulation we considered the case in which the intruder has high initial energy as compared to other normal nodes. In LEACH cluster heads are being selected based on the residual energy of various nodes. Since attacker is having higher initial energy so it becomes one of the cluster heads in the first round and even in later rounds, as it is not consuming any energy for data transmission. Hence it becomes cluster head in almost all the rounds. After becoming cluster head it receives data from all of its cluster members, aggregate it and later on do not forward the data to the base station.

D. Gray Hole Attack

In Gray Hole attack [8] initially, a malicious node exploits the LEACH protocol to advertise itself as having a high probability to

become a cluster head, with the intention of intercepting packets, next, the node drops the intercepted packets with a certain probability. A Gray Hole may exhibit its malicious behavior in multiple ways. It simply drops packets coming from certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of Gray Hole attack is a node behaves maliciously for some particular time duration by dropping packets but may switch to normal behavior later or it may packets of certain packet ID and forward the other packets. A Gray Hole may also exhibit a random behavior also in which it drops some of the packets randomly while forwarding other packets, thereby making its detection even more difficult.

Table 1 Routing protocol threats in sensor networks [11]

Threats	Description
Selective forwarding	Malicious node block the passage of all or selective messages.
Wormholes	Two malicious nodes in different parts of the network colluding to understate their distance from each other to deceive other nodes.
Sybil	Malicious node illegally claims multiple identities
Sinkhole	Fool large number of nodes that compromised node has the high quality route
Hello floods	Malicious node with larger enough transmission power, flood Hello packets to far nodes to deceive them to use false route, to cause confusion to the networks.
Acknowledgement spoofing	Spoof Acknowledgement message to sender with reverse information.
Cloning	Malicious node clones the requests, thus inducing an alternative data flow to itself.

III. SECURE AND ENERGY EFFICIENT ROUTING TECHNIQUES IN WSN

In this paper [1], The authors propose two secure and efficient data transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the identity-based digital signature (IBS) scheme and the identity-based online/offline digital signature (IBOOS) scheme, respectively. In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing domain. SET-IBOOS further reduces the computational overhead for protocol security, which is crucial for WSNs, while its security relies on the hardness of the discrete logarithm problem. The authors show the feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks. In [2], energy efficient routing protocols are classified into four main schemes: Network Structure, Communication Model, Topology Based and Reliable Routing. The routing protocols belonging to the first category can be further classified as flat or hierarchical. The routing protocols belonging to the second category can be further classified as Query-based or Coherent and non-coherent based or Negotiation-based. The routing protocols belonging to the third category can be further classified as Location-based or Mobile Agent-based. The routing protocols belonging to the fourth category can be further classified as QoS-based or Multipath based. Then, an analytical survey on energy efficient routing protocols for WSNs is provided. In [3], an efficient key distribution scheme is provided which is useful to secure data-centric routing protocols in Wireless Sensor Networks. Similar to these routing protocols, the proposed scheme bootstraps secure key distribution with a centralized process which gives a multi-level hierarchical organization to WSNs. These two types of keys are useful to secure respectively data request diffusion and data forwarding through multi-hop routing paths. The authors in [4] proposed an optimization model for network management in multihop Wireless Sensor Networks (WSNs). Here, the authors develop a distributed, braided multipath algorithm to deliver the information from the information sources (targets) to the Base stations (sinks) giving the network the ability to adapt to changes or failures. The Base Stations are robust nodes with capabilities for positioning themselves and communicating outside the network, which grants them the benefit of knowing other Base Stations' position in the area of interest. Targets are nodes that generate information and need a fixed amount of bandwidth to convey this information to a Base Station. To increase network's resilience, the devices within the network will try to create multiple paths from

the beginning trying to reach at least one Base Station. The model is solved through a heuristic algorithm based on the nearest neighbor and minimum hop concepts. SIVA D. MURUGANATHAN et. al. [5] proposed a centralized routing protocol called Base-Station Controlled Dynamic Clustering Protocol (BCDCP), which distributes the energy dissipation evenly among all sensor nodes to improve network lifetime and average energy savings. Wireless sensor networks consist of small battery powered devices with limited energy resources. In [6], the author described three new protocols for wireless sensor networks. One of these protocols, PEGASIS, is a greedy chain protocol that is near optimal for a data gathering problem in sensor networks. PEGASIS outperforms LEACH by eliminating the overhead of dynamic cluster formation, minimizing the distance non-leader nodes must transmit, limiting the number of transmissions and receptions among all nodes, and using only one transmission to the BS per round. Nodes take turns to transmit the fused data to the BS to balance the energy depletion in the network and preserve the robustness of the sensor web as nodes die at random locations. In [7], the authors have proposed LNT: a Logical Neighbor Tree for secure group management that can be applied to a homogeneous WSN network with a resource-constrained group controller. The scheme alleviates the group controller's task by constructing a logical neighbor tree that helps deliver the rekeying messages. Performance analysis has shown that our scheme outperforms some previously well-known schemes in terms of computation, communication and storage costs. LNT scheme can be improved by replacing the ECC-based digital signature scheme by a more lightweight method of authentication such as the use of a key-chain. In [9], the authors have planned a pragmatic energy model alongside the trust based secure and energy-efficient clustering method for WSNs using HBMA. The authors also argue that our energy model is the most apposite for real scenario, as it covers all the basic functionalities of a sensor node. For harmonizing the energy expenditure among cluster heads, clusters nearer to the base station are of smaller sizes than remote ones from the base station. Hence cluster heads closer to the base station preserves some energy. For opting an appropriate cluster head the authors have also introduced the most desirable TRUST mechanism, which avoid the malicious node to be cluster head [9]. The authors in [10] have proposed an energy-efficient data collection in wireless sensor networks (WSNs) that is based on an integration of the clustering and compressive sensing (CS). The authors introduced the integration of the CS with clustering to benefit from the power saving offered by the two techniques. The authors refer to our scheme as clustered-base CS (CCS). The resulting CS measurement matrices in CCS are in the form of block diagonal matrices (BDMs). This paper [12] presents novel deterministic and hybrid approaches based on Combinatorial Design for deciding how many and which keys to assign to each key-chain before the sensor network deployment. Secure communications in wireless sensor networks operating under adversarial conditions require providing pairwise (symmetric) keys to sensor nodes. For secure communication either two nodes have a key in common in their key-chains and they have a wireless link between them, or there is a path, called key-path, among these two nodes where each pair of neighboring nodes on this path have a key in common. Length of the key-path is the key factor for efficiency of the design. In particular, Balanced Incomplete Block Designs (BIBD) and Generalized Quadrangles (GQ) are mapped to obtain efficient key distribution schemes.

IV. CONCLUSION AND FUTURE WORK

A sensor network is composed of many sensor nodes which are deployed in a wide area. These nodes form a network by communicating with each other either directly or through other nodes. One or more nodes among them will serve as sink(s) that are capable of communicating with the user either directly or through the existing wired networks. Wireless sensor networks can be utilized in a broad variety of applications ranging from battlefield surveillance in military, through remote patient monitoring in medicine to forest fire detection in environmental applications. Majority of WSN applications require at least some level of security. In order to achieve the needed level, secure and robust routing is necessary. Secure data transmission is a critical issue for wireless sensor networks (WSNs). The future work is to design a routing protocol which is secure and reliable. To secure the transmission, we can use encryption methods and for reliability we can use hierarchical routing or cluster based wireless sensor network. Clustering is an effective and practical way to enhance the system performance of WSNs. Cluster-based data transmission in WSNs has been investigated by researchers to achieve the network scalability and management, which maximizes node lifetime and reduce bandwidth consumption by using local collaboration among sensor nodes. In a cluster-based WSN (CWSN), every cluster has a leader sensor node, regarded as cluster head (CH). A CH aggregates the data collected by the leaf nodes (non-CH sensor nodes) in its cluster, and sends the aggregation to the base station (BS).

REFERENCES

[1] Huang Lu, "Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks", IEEE TRANSACTIONS ON PARALLEL AND

DISTRIBUTED SYSTEMS, VOL. 25, NO. 3, MARCH 2014 pp. 750- 761.

[2] Nikolaos A. Pantazis, Stefanos A. Nikolidakis and Dimitrios D. Vergados, "Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey" IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 2, SECOND QUARTER 2013 pp. 551- 591.

[3] Abderrahmen Guermazi, "An Efficient Key Distribution Scheme to Secure Data-Centric Routing Protocols in Hierarchical Wireless Sensor Networks", The 2nd International Conference on Ambient Systems, Networks and Technologies (ANT) Procedia Computer Science, 2011, pp 208–215.

[4] Carlos Velasquez, " Multipath Routing Network Management Protocol for Resilient and Energy Efficient Wireless Sensor Networks", Information Technology and Quantitative Management, ITQM 2013 Procedia Computer Science 17, 2013, pp. 387 – 394.

[5] SIVA D. MURUGANATHAN, DANIEL C. F. MA, ROLLY I. BHASIN, "A Centralized Energy-Efficient Routing Protocol for Wireless Sensor Networks", IEEE Radio Communications, March 2005.

[6] Stephanie Lindsey, Cauligi Raghavendra," Data Gathering Algorithms in Sensor Networks Using Energy Metrics", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 13, NO. 9, SEPTEMBER 2002.

[7] Omar Cheikhrouhoua, Anis, "LNT: a Logical Neighbor Tree for Secure Group Management in Wireless Sensor Networks", The 2nd International Conference on Ambient Systems, Networks and Technologies (ANT), Procedia Computer Science 5, 2011 pp. 198–207.

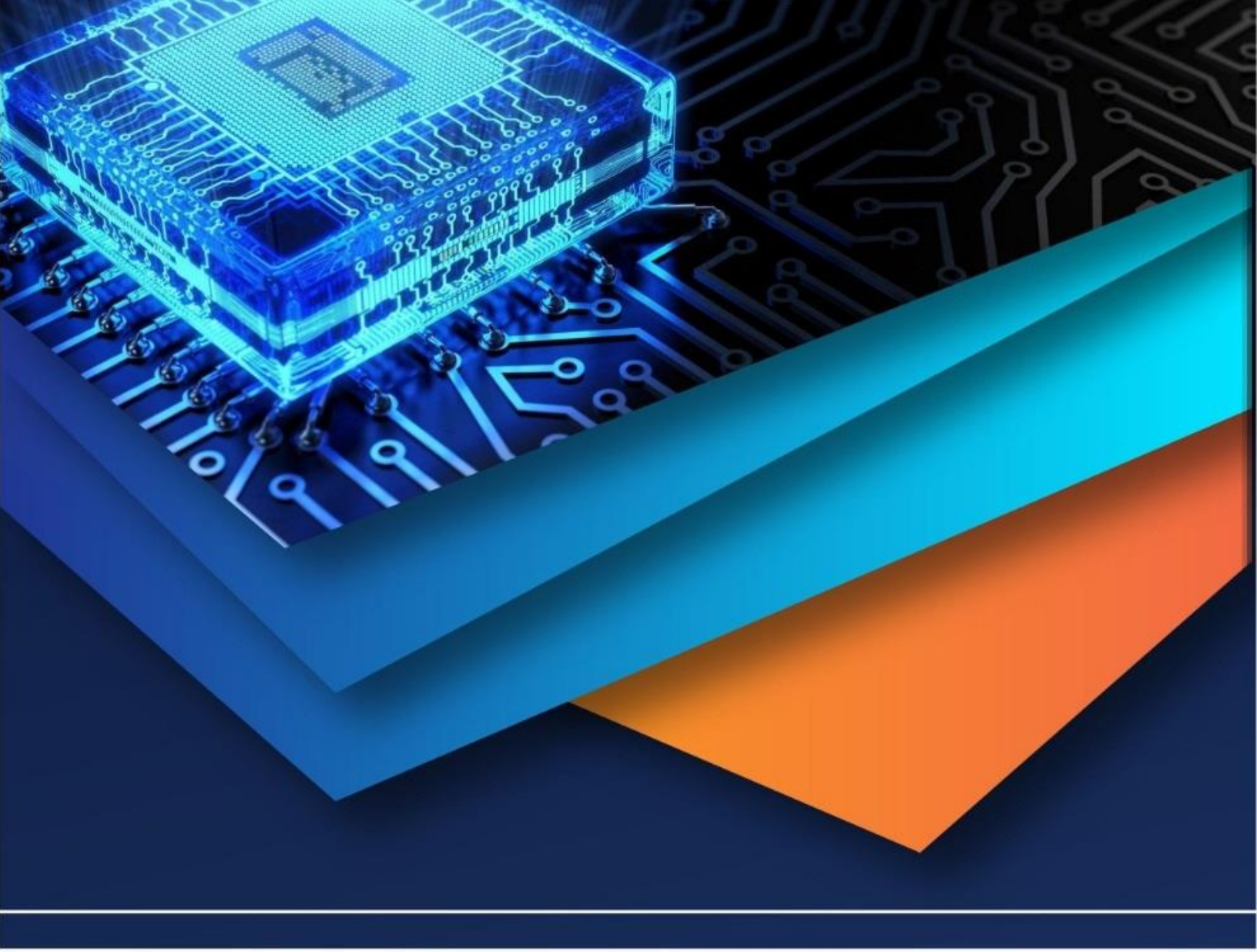
[8] Meenakshi Tripathi,M.S.Gaur,V.Laxmi, "Comparing the Impact of Black Hole and Gray Hole Attack on LEACH in WSN", The 8th International Symposium on Intelligent Systems Techniques for Ad Hoc and Wireless Sensor Networks (IST-AWSN) Procedia Computer Science 19, 2013.

[9] Rashmi Ranjan Sahoo, Moutushi Singh, Biswa Mohan Sahoo, "A Light Weight Trust Based Secure and Energy Efficient Clustering in Wireless Sensor Network: Honey Bee Mating Intelligence Approach", International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA), 2013.

[10] Minh Tuan Nguyen and Nazanin Rahnavard , "Cluster-Based Energy-Efficient Data Collection in Wireless Sensor Networks utilizing Compressive Sensing", IEEE Military Communications Conference, 2013.

[11] Mostafa I. Abd-El-Barr Maryam M. Al-Otaibi Mohamed A. Youssef, "WIRELESS SENSOR NETWORKS- PART II: ROUTING PROTOCOLS AND SECURITY ISSUES", IEEE, May 2005.

[12] Seyit A. Camtepe, Bulent Yener, "Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks", IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 15, NO. 2, APRIL 2007.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY