International Journal of Engineering Research and Development
e-ISSN: 2278-067X, **p**-ISSN: 2278-800X, www.ijerd.com
Volume 7, Issue 1 (May 2013), PP. 86-93

Reduce Load at Base Station by Node Authentication Using Intra-Cluster Formation in Wireless Sensor Network

Keyur N. Zala[1], Diwan Raimagia[2], J. N. Rathod[3]
[1,2,3] Atmiya Institute of Technology & Science, Rajkot, Gujarat, India.

Abstract:- Area of Wireless sensor networks is very wide such as military, environment, agriculture and so on. Security is critical to sensor networks deployed in hostile location, such as military field and security observation. The need of security on digital environment has appeared. Various cryptographic algorithms has been offered to transmit data in a secure environment. In this study, focus is drawn on load to base station while implementing public key cryptography. We proposed Hierarchical framework for key distribution. Here main function of cluster head is to distribute key to cluster nodes and decrypt data from nodes to cluster head. With our frame work load on base station is reduced, result shows that load on base station after clustering of data is much reduced and malicious nodes are dropped by cluster head. Here Public-key encryption i.e. RSA, Chinese Remainder Theorem is implemented**.**

Keywords:- Base Station (BS), Cluster Head (CH), Member node (MCH),RSA, RSA with CRT, AODV, Bit rate, Packet delay, Number of packets.

I. INTRODUCTION

All Most previous research efforts consider homogeneous sensor networks, where all sensor nodes have the same configuration and capabilities. However, a homogeneous ad hoc network suffers from poor fundamental limits and performance. Research has verified its performance bottleneck both theoretically and through simulation experiments and test bed measurements. Several recent works studied Heterogeneous Sensor Networks (HSNs), where sensor nodes have different capabilities in terms of message passing, calculation, energy supply, storage capability space, reliability and other aspects.

In a wireless sensor network, physical security of wireless links is virtually impossible because of the broadcast nature and resource limitation on sensor nodes and uncontrolled environments where they are left unattended [1]. Consequently security attacks on information flow can be widespread, e.g. passive interception of data transmission, active injection of traffic and overloading the network with garbage packets. Modification of information is possible because of the nature of the wireless channels and uncontrolled node environments. An opponent can make use of these natural impairments to modify information and also render the information unavailable. Wireless sensor networks also have the general security requirements of integrity, availability, confidentiality, authentication, and non-repudiation. These security requirements can be provided by a key distribution mechanism [2] with requirements of scalability, efficiency, key connectivity and resilience.

Wireless networks are usually more vulnerable to various security threats as the unguided communication medium is more susceptible to security attacks than those of the guided transmission medium. For listening secretly, the broadcast nature of the wireless communication is a simple candidate. In most of the cases various security issues and threats related to those we consider for wireless ad hoc networks are also applicable for wireless sensor networks. These issues are well- ascertained in some past researches and also a number of security schemes are already been proposed to fight against them [4, 6]. However, the security mechanisms devised for wireless ad hoc networks could not be applied directly for wireless sensor networks because of the architectural disparity of the two networks. While ad hoc networks are unsupervised, active topology, peer to peer networks formed by a collection of mobile nodes and the centralized entity is absent; the wireless sensor networks could have a command node or a base station. The design aspect of wireless sensor network could make the employment of a security schemes little bit easier as the base stations or the centralized entities could be used extensively. However, the major challenge is induced by the constraint of resources of the minute sensors. Generally, sensors are probable to be deployed arbitrarily in the enemy territory (especially in military reconnaissance scenario) or over dangerous or hazardous areas. Therefore, even if the base station (sink) resides in the friendly or secure area, for compromising the sensor nodes are need to be protected. Further load and complexity increases at base station because of key distribution to all sensors, and decryption of data and find malicious node by base station. All this leads to increase in load to base station.

II. ATTACKS IN WIRELESS SENSOR NETWORK

Attacks against wireless sensor networks could be mostly classified from two different points of view [7-11]. One is against the security mechanisms and another is against the basic mechanisms (like routing mechanisms). Below are some of the major attacks described, which occurs in wireless sensor networks.

A. Denial of Service

Denial of Service is produced by the unintentional failure of nodes or malicious action. The simplest Denial of Service attack tries to weaken the resources available to the target node, by sending more and more unnecessary packets and thus prevents genuine network users from accessing services or resources to which they are entitled [3]. Denial of Service attack is meant not only for the adversary’s attempt to destabilize, disorder, or devastate a network, but also for any event that diminishes a network’s capability to provide a service. Several types of Denial of Service attacks in different layers might be done in wireless sensor networks. At physical layer the Denial of Service attacks could be congestion and tampering. At link layer, collision, collapse, wrong. At network layer, ignore and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and resynchronization. The mechanisms to prevent Denial of Service attacks include payment for network resources, reposition, well-built authentication and detection of traffic.

B. Attacks on information in Transit

In a sensor network, sensors monitor the changes of specific parameters or values and report to the sink according to the requirement. The information in transit may be changed, spoofed, replayed again or mislaid while sending the report. As wireless communication is susceptible to eavesdropping, any attacker can observe the traffic flow and get into action to suspend, intercept, alter or fabricate packets thus, provide wrong malicious information to the base stations or sinks. During transmission, as sensor nodes usually have short range of transmission and limited resource, an attacker with high processor and better communication range could assail several sensors simultaneously at same time to modify the actual data.

C. Sybil Attack

In Wireless Sensor Network mostly, the sensors might need to work together to complete a job, hence they can use the subtasks distribution and redundancy of information. In this case, a node can act as more than one node using the identities of other genuine nodes (Figure 1). This type of attack where a node forges the identities of more than one node is the Sybil attack [5]. Sybil attack tries to mortify the integrity of data, security and resource consumption that the distributed algorithm attempts to accomplish. Sybil attack can be done for attacking the distributed storage, data aggregation, selection, routing mechanism, reasonable resource allocation and misconduct detection. Basically, wireless ad hoc networks are vulnerable to Sybil Attacks. However, as WSNs can have some sort of base stations or gateways, this attack could be prohibited using efficient protocol.

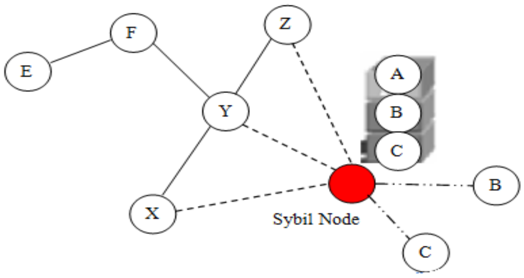

Fig. 1 Sybil Attack

D. Blackhole/Sinkhole Attack

In this attack, a malicious node acts as a black hole to attract all the traffic in the sensor network. Particularly in a flooding based protocol, the attacker waits and listens to requests for routes then replies to the target nodes that it contains the high value or shortest path to the base station (BS). Once the malicious device has been able to insert itself between the communicating nodes (i.e. sink node and sensor node), it is able to do anything with the packets passing between them. Further, this attack can affect still the nodes those are considerably distant from the base stations. Fig 2.shows the conceptual view of a blackhole/sinkhole attack.

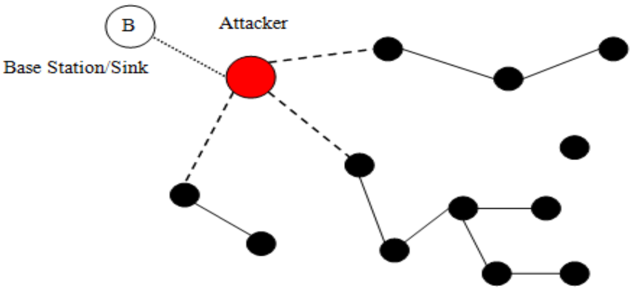

Fig. 2 Conceptual view of blackhole attack

E. Hello Flood Attack

This attack uses HELLO packets as a weapon to convince the sensors in WSN. In this kind of attack an attacker with a high radio transmission range and processing power sends HELLO packets to a number of sensor nodes which are isolated in a large area within a WSN. The sensors are thus convinced that the antagonist is their neighbour. As a result, while sending the information to the base station, the victim nodes try to go all the way through the attacker as they know that it is their neighbour and are ultimately spoofed by the attacker.

F. Wormhole Attack

Wormhole attack is a critical attack in which the attacker records the packets (or bits) at one location in the network and tunnels those to another location. The tunnelling or retransmitting of bits could be done selectively.

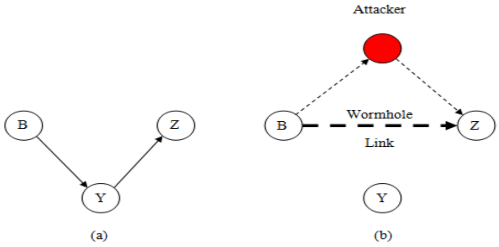

Fig. 3 Wormhole attack

Wormhole attack is a significant threat to wireless sensor networks, because; this kind of attack could be performed even at the initial phase i.e. discovery of neighbor nodes information. Hence Wormhole attack does not require compromising a sensor in the network. Fig 3 (a/b) shows a situation where a wormhole attack takes place. When a node B (base station or any other sensor) broadcasts the routing request packet, the attacker receives this packet of information and replays it in its neighborhood. Each adjacent node receiving this replayed packet will consider itself to be in the perimeter range of Node B, and hence will mark this node as its parent. Thus, even if the victim nodes are multi hop at a distance from B, attacker in this case convinces victim node that B is only a single hop away from them, thus creates a wormhole attack.

III. OVERVIEW OF ENCRYPTION STANDARDS

A. Public Key Encryption

There are a lot of secret key algorithms. The most commonly used three algorithms are Caesar shifts, DES and RSA. One of the most important opinions about public-key encrypting systems is that these systems can never provide unconditional security. Because other side can find value A obtaining B=ek(A), by using rule EK by using encrypted expression B. A expression is decrypted form of expression B. Hence, studies are made on computable security of public-key encryption standard algorithm. It is preferred that suitable public-key algorithm is easily computable and inverse transforming function is also hardly computable. This is generally called infectivity.

As a result, ek is chosen to be an injective function as it preserves distinctness. Injective functions have important role on the encrypting the message. It uses this kind of functions to develop public-key encryption systems. It is not enough that we have an injective function, if we talk about public-key encrypting systems. If ek continues to be injective function for endorsed persons, it cannot be possible that they decrypt the encrypted data. Also by eliminating the injective function, the owner of the text be able to reach to the original text easily. This causes the requirement that the owner of the text must be able to find the inverse of ek rule through extra information that she/he knows, by using a kind of secret channel.

Injective functions are used in the RSA systems. But formal person can obtain easily the rule of inverse transforming through the private key. Before talking about details of RSA, it is useful to explain two subjects about modular arithmetic and numbers theory.

B. RSA Algorithm

The security of the RSA cryptosystem depends on the difficulty of factoring large integers. The longer the key, the higher the work factor the cryptanalyst has to pact with. For breaking the system by exhaustive search of the key space, the work factor is exponential in the key length. Secrecy comes from having a strong (but public) algorithm and a long key.

C. RSA with CRT Algorithm

A major difference between the RSA scheme and cryptosystems based on the discrete logarithm problem is the fact that the modulus used in the RSA encryption scheme is the product of two prime numbers. This allows utilizing the Chinese Remainder Theorem (CRT) in order to speed up the private key operations. The usage of the CRT for RSA decryption is well known from mathematical point of view. But for a hardware implementation, special multiplier architecture is necessary to meet the requirements for efficient CRT-based decryption.

IV. CLUSTER FORMATION

A Current Clusters are formed in an HSN. We have designed an efficient clustering scheme for HSNs. Because of the page limit, we will not describe the details of the clustering scheme. Let us assume that each H-sensor can communicate directly with its neighbor H-sensors (if not, then relay via L-sensors can be used). All H-sensors form a basic support in an HSN [12]. After cluster formation, an HSN is alienated into multiple clusters, where H sensors serve up as the cluster heads.

An illustration of the cluster formation is shown in Fig 4 where the small squares are L sensors, large rectangular nodes are H-sensors, and the large square at the bottom-left corner is the sink.

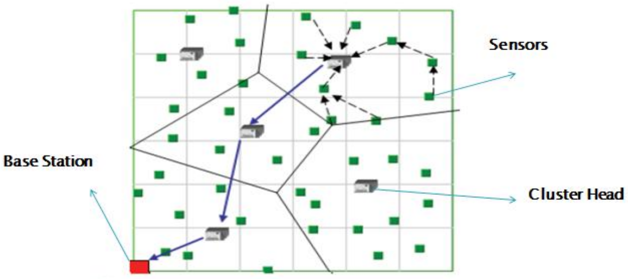

Fig. 4 Cluster Formation in an HSN

In wireless sensor networks, a cluster algorithm is a good option to reduce redundant data transfer and organize nodes effectively for long life [10]. In this paper we implement and evaluate a new hierarchical and flexible clustering algorithm on the middleware layer based paradigm.

In general, in order to solve all the problems, there needs a novel clustering algorithm for sensor nodes to aggregate data so as to reduce redundant transmissions, perform localized computation so as to increase non-volatile information throughput, and optimize energy consumption so as to prolong the system lifespan.

V. PROPOSED ARCHITECTURE

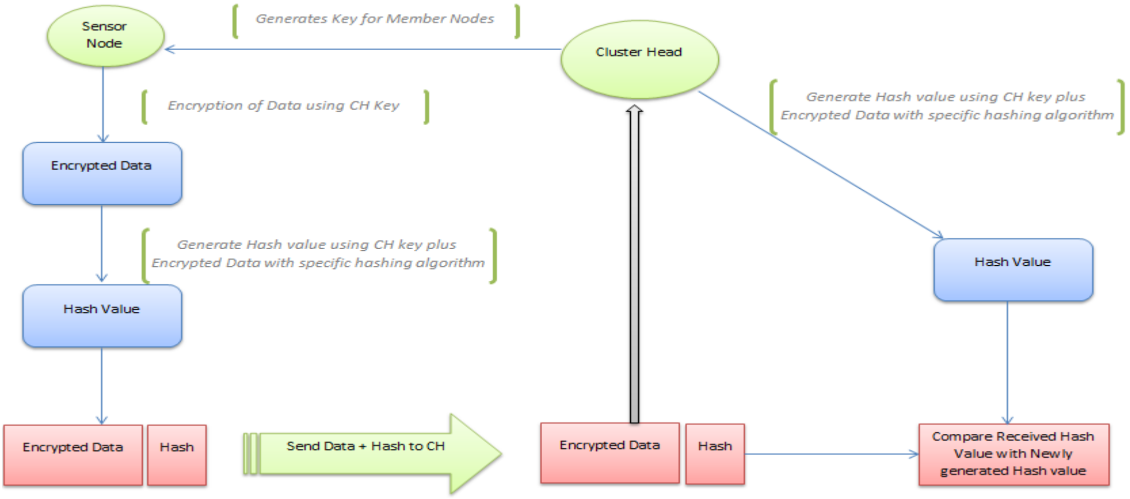
Sensor Node
Generates Key for Member Nodes
Cluster Head
Encryption of Data using CH Key
Encrypted Data
Generate Hash value using CH key plus Encrypted Data with specific hashing algorithm
Hash Value
Generate Hash value using CH key plus Encrypted Data with specific hashing algorithm
Hash Value
Encrypted Data
Hash
Send Data + Hash to CH
Encrypted Data
Hash
Compare Received Hash Value with Newly generated Hash value

Fig. 5 Authentication of Nodes by Cluster Head

Here, in these architecture two levels of authentication is proposed for authenticating nodes to CH and authentication of CH by BS (Base station) is done.

As shown in figure 5, initially cluster head member nodes sense data, after sensing, data is encrypted with RSA or RSA with CRT algorithm using public key of CH. After encryption of data, encrypted data and key are combined to generate hash value using any hashing algorithm say MD5 or SHA.

After generating hashing, encrypted data and hash value are combined and send it of CH. At Cluster head hash value is generated using private key. Now newly generated hash at CH and hash send by MCH are compared, if hash value is found incorrect node is considered to be malicious and nodes are not considered as member of CH and instead of forwarding data to BS, malicious nodes are dropped at CH hence work load of BS is reduced

As shown in figure 6, Encrypted data at cluster head (CH) and using Public key of BS generates hash value using any hashing algorithm say MD5 or SHA.

After generating hashing, encrypted data and hash value are combined and send it of BS. At Base Station hash value is generated using private key. Now newly generated hash at BS and hash send by CH are compared, if hash value is found incorrect CH is considered to be malicious and Cluster Head are not considered as member of BS and instead of accepting data from CH, malicious CH are dropped at BS. After node authentication data are decrypted and considered as valid.

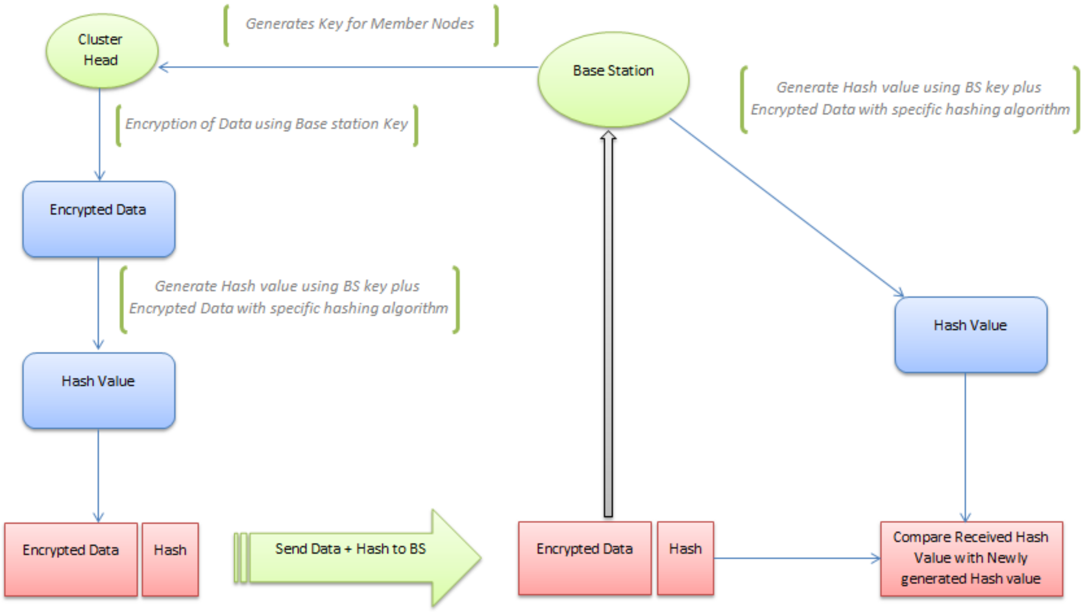
Cluster Head
Generates Key for Member Nodes
Base Station
Encryption of Data using Base station Key
Encrypted Data
Generate Hash value using BS key plus Encrypted Data with specific hashing algorithm
Hash Value
Generate Hash value using BS key plus Encrypted Data with specific hashing algorithm
Hash Value
Encrypted Data
Hash
Send Data + Hash to BS
Encrypted Data
Hash
Compare Received Hash Value with Newly generated Hash value

Fig. 6 Authentication of Cluster Head by Base Station

VI. EVALUATION OF PROPOSED FRAMEWORK

We had taken 100 nodes for simulation. 6 clusters are used. AODV routing protocols is used for routing process. We had simulated the same scenario in three different environments using three different encryption algorithms RSA, and RSA+CRT. For generating hash value MD5 algorithm is used.

TABLE I Environment Variables And Its Associated Values Used In Experiment

No.	Environment Variables	Associated Values
1	Simulation Tool	Cygwin+Ns-Allinone-2.28
2	Bandwidth of HSN Environment	1MB
3	Initial Energy	100 Joules
4	Antenna Type	Omni Direction
5	Base Protocol	AODV
6	Total Number of Nodes	100
7	Encryption Standards	RSA and RSA with CRT
8	Hashing Algorithm	MD5
9	Optimal number of cluster heads	6
10	Simulation time	3600s

We have improved three primary performances using the Route-Driven methods. Using routing driven approach we had achieved three things.

Encryption methods have been established for the data transmission from sensor nodes to the cluster head, there by the malicious data will be blocked in the cluster head itself thereby reducing the unnecessary malicious data traffic from cluster head to base station.

For the Sensor nodes and Cluster head encryption, key generation parameters are distributed dynamically within the cluster itself rather than getting common key from the base station. This reduces the unnecessary overhead of the base station.

Dynamic key generation and Route Driven Encryption have been established using three algorithms viz. RSA Algorithm and RSA with CRT Algorithm. The Performance Analysis for these Algorithms is tabulated below.

TABLE III Performance Analysis

Parameters	RSA Algorithm	RSA with CRT Algorithm
Key Size	1024 bits	1024 bits
Security	High	Highest
Approach	Asymmetric	Asymmetric
Encryption	Slow	Fastest

A. Energy Consumption

Based on the Simulation Analysis, the Energy consumption at base station increases as number of nodes increases, but after formation of cluster result shows that performance in this case, energy consumption is very less as workload at base station reduces because of cluster formation key generation during encryption and acknowledgement to nodes reduces. All the data is being encrypted both in cluster head and base station is represented in the graphical analysis.

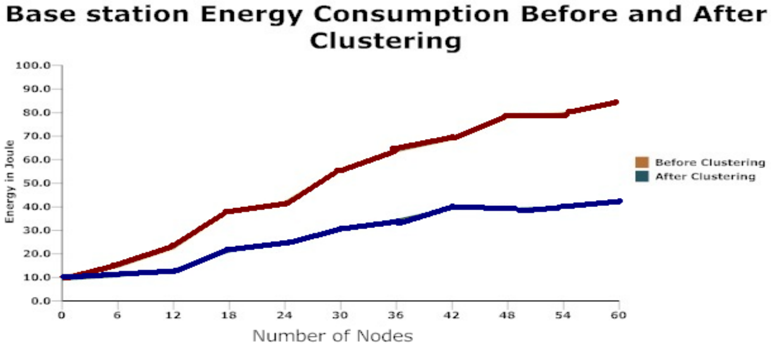

Fig. 7 Energy Consumption at Base Station

B. Malicious Packet

Based on the Simulation Analysis, the packet received at base station must be secure i.e. packets send by malicious nodes must be dropped. Thus because of two levels of hierarchy, majority of work of removing malicious data is done by cluster head instead of base station, base station only checks data encrypted by cluster head. Hence as shown in graph packets received is reduced at base station as malicious packets are dropped by cluster head.

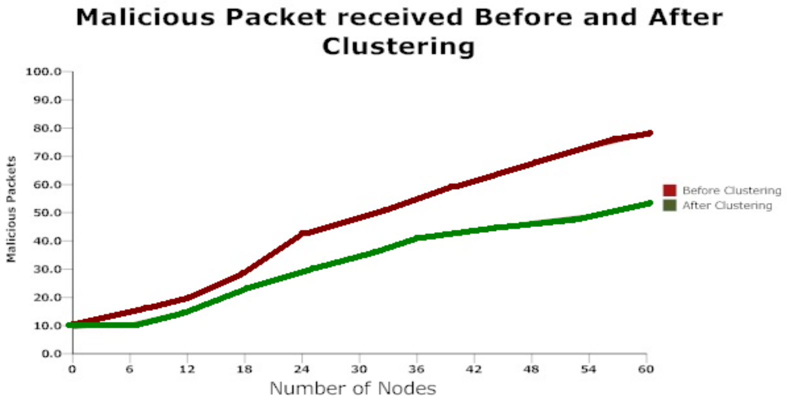

Fig. 8 Malicious Packet

C. Performance speedup of Base Station

This Simulation Analysis Chart shows the number of packets received in the case of RSA, RSA with CRT Algorithms under the simulation environment. The Performance results show that during simulation as number of nodes increases the work load of base station increases drastically as base station needs to generate key during encryption process, performs encryption of packets, check whether packets received is malicious or not, validate new nodes etc. As load increases to base station, performance reduces as shown in figure 7; hence clustering is the best option for reducing work load to the base station. As majority of work done occurs at cluster head, hence performance at base station increases.

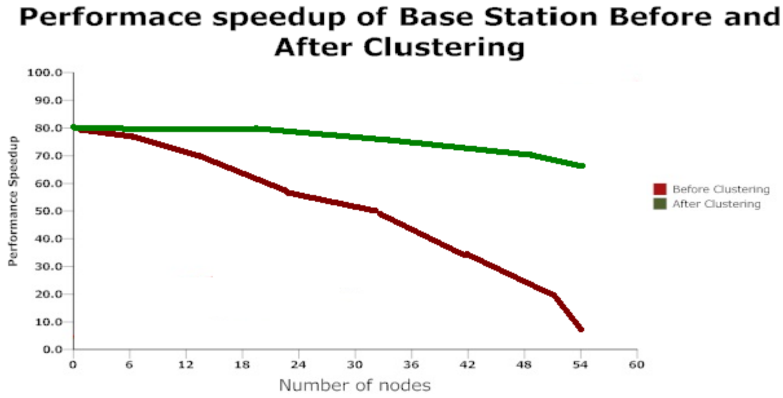

Fig. 9 speedup ratio with number of nodes at base station

VII. CONCLUSION

Through simulations, we have compared the performances of Energy consumption at base station, malicious packet received at base station, Load ratio with number of nodes at base station. Result shows that cluster formation is better as compared to direct packet sending and receiving at base station as majority of work is distributed at cluster head.

REFERENCES

[1]. Asmae BLILAT, Anas BOUAYAD, Nour el houda CHAOUI, Mohammed EL GHAZI. Wireless sensor network: security challenges.

[2]. Md. Iftekhar Salam, Pardeep Kumar, HoonJae Lee. An Efficient Key Pre-distribution Scheme for Wireless Sensor Network

[3]. Using Public Key Cryptography.

[4]. Y.Wei, L. Paul, J. Havinga, “How to secure a Wireless Sensor Network” 0-7803-9399-6/2005.

[5]. A. D. Wood and J. A. Stankovic. (2002) Denial of service in sensors networks, Computer, 35(10) pp 54-62.

[6]. Ren Xiu – li, Yang Wei Method of detecting the Sybil Attack Based on Ranging in Wireless Sensor Network.

[7]. C. Y Chong, and S. P. Kumar. (2003) Sensor networks: evolution, opportunities, and challenges, Proceedings of the IEEE, 91(8), pp 1247-1256.

[8]. P. A. Szewczyk, R. Tygar, J. Wen, V. Culler, “SPINS: Security protocols for sensor networks, Wireless Networks”, 8(5) pp 521-534.

[9]. K. J. Rabiner, W. Balakrishnan, “Adaptive protocols for information dissemination in wireless sensor networks”, in Proceedings of 5th ACM/ IEEE-MOBICOM’99 conference.

[10]. Hamed EL_afandi . An Intellig ent Wireless Ad hoc Routing Protocol. In University of Wisconsin_Milwaukee, 2006.

[11]. C.Schurgers and M. B. Srivastava. Proceedings of IEEE MlLCOM," Energy efficient routing in wireless sensor networks", 2008.

[12]. Ding, P., Holliday, J., and Celik, A. Distributed energy hierarchical clustering for wireless sensor networks. In Proceedings ofhe IEEE International Conference on Distributed Computing in Sensor Systems(DCOSS05) (June 2005).