HEF Clustering for Secure and Efficient Data Transmission in CWSN

Kesia Salimon
Department of Electronics and Communication Engineering, Dhanalakshmi Srinivasan College of Engineering, Coimbatore, India

R. Lavanya
Department of Electronics and Communication Engineering, Kongu Engineering College, Erode, India

B. Mathivanan
Department of Electronics and Communication Engineering, Dhanalakshmi Srinivasan College of Engineering, Coimbatore, India.

ABSTRACT
Among the modern wireless networks, wireless sensor network plays a prominent role. Bunch reduces the general energy consumption. In this paper HEF (High Energy First) bunch protocol is employed. This protocol provides improved network time period since the energy level of the nodes are considered while choosing the cluster head. The cluster area is fashioned dynamically and sporadically. The cluster heads are usually having more resources (generally energy) on comparison with other nodes in the cluster. We tend to propose a globally trust management theme that enhance security in WSNs. In this trust management scheme, trust model takes 2 methodologies, trust from direct observation methodology and trust from indirect observation method. In direct observation methodology observer node gets trust value by exploiting theorem reasoning. On the other hand, with indirect observation trust value is obtained from neighbor nodes of the observer node. The trust value for this methodology is based on Dempster-Shafer theory. Combining these 2 trust models, we tend to get a lot of correct trust values that results the effectiveness of our methodology.

Keywords
Wireless Sensor Networks (WSN), High Energy First (HEF), Dempster -Shafer theory, Harmonic Search Algorithm (HSA), Cluster Head (CH), Base Station (BS), Cluster based WSN (CWSN)

1. INTRODUCTION
The sensor nodes concerned in the network is capable of measuring and aggregating info concerning its surroundings. The collected knowledge ought to be delivered to the destination that is capable of processing the received knowledge [1]. The wireless sensor network takes an open medium and therefore the sensor nodes take a distant distribution. These options of the network provide the chance of diverse attacks. So while designing a sensor network, care should be taken to ensure the security.

2. RELATED WORKS
Our planned system has the contributions like identification and replacement of a delicate collusion attack against IF based totally named systems that reveals a severe vulnerability of IF algorithms; 2) distinctive methodology for estimation of devices' errors that is effective in sensing wide range of faults related to data transfer and that are not susceptible to the drawn attacks; 3) low cost and powerful aggregation methodology galvanized by the MLE, that utilizes the associated estimate of the noise parameters obtained by considering the boundary limits 4) augmented IF schemes able to defend against delicate collusion attacks by providing an initial estimate of trust of sensors involved in the network considered.

3. SYSTEM MODEL
We interpret trust as the degree of belief that a node performs of course. We have a tendency to conjointly acknowledge uncertainty in trust analysis. Supporting this interpretation, we have a tendency to propose a trust management scheme to reinforce the protection of WSNs [2]. We have a tendency to use unsure reasoning to derive trust values. Trust from direct observation and trust from indirect observation. With direct observation from associate observer node, the trust worth comes, that could be a style of unsure reasoning once the total likelihood model may be outlined.

On the opposite hand, with indirect observation from neighbor nodes of the observer node the trust worth comes, that is associated with other style of unsure reasoning once the proposition of interest may be derived by an indirect methodology. We have to conjointly implement the information security, by encrypting and decrypting the information.

3.1 Modules Involved
The system can be divided mainly as following modules based on its performance features. Analysis of the modules is required.

- Communication Model
- Trust Model
- Direct Trust Model
- Recommended Trust Model
- Trust Value Analyzer
- Eliminate the Hacker Node
- Deployment of sensor
- Cluster formation
- Cluster head rotation
- Security

3.1.1 Communication Model
Initially we are inserting nodes within the network and that we opt for a source and destination. If the source has no route to the destination, then source A initiates the route discovery in an on-demand fashion. When generating RREQ, node searches its own neighbor table to seek out if there is any nearer neighbor node toward the destination node. If a more in-depth neighbor node is accessible, the RREQ packet is forwarded there to node. If no nearer neighbor node is available the RREQ packet is flooded to all or any neighbor nodes. Once destination receives the RREQ, it will generate RREP and it will send an equivalent path. Finally we have to establish the route for information traffic.

3.1.2 Trust Model
Trust value is generated by two different value generation processes.

3.1.3 Direct Trust Model
The nodes can monitor other node by one hop neighbors. This trust value is calculated by nodes parameters like node's energy state and sequence range. Hacker node can show continually high energy state and high sequence range for knowledge forwarding. Based on this, trust value can be generated.

3.1.3 Indirect Trust Model
After finding the route, source can send request to any or all the nodes. It can represent the neighbor nodes and update the trust price of its neighbors by which value is passed to source node.

3.1.4 Trust Value Analyzer
Source node can get trust price from each direct and indirect trust price models. Based on these trust values, it'll take a choice.

3.1.5 Eliminate the Hacker Node
Finally source node can track the hacker node. It won't select a route which has a hacker node. It'll choose alternate route for data forwarding. It'll check hacker details sporadically.

3.2 Deployment of Sensor
Deployment of the nodes in a wireless sensing element network to satisfy continuous sensing along with extended network time period and maintaining uniform coverage within the sensing region is the major challenge in wireless sensing element networks.

Various architectures and node deployment methods [3] are developed for wireless sensing element network, relying upon the necessity of application [4]. Node preparation in wireless sensing element network is application dependent and might be either settled or randomized.

Sensor networks area unit is typically deployed in a sensing field to gather helpful info from it. Typically the preparation of sensing element network [5] may be a labor intensive and cumbersome task because the planet influences trigger bugs or degrade performance during an approach that has not been ascertained throughout pre-deployment. This can be helpful in the explaining the functions of the sensing element network which is powerfully influenced by the important unit that controls the output of the sensors.

There are unit bound pertinent problems concerning the sensing element network preparation. An important demand is that the presence of a minimum of one data sink node, particularly entry, at that data transmitted from the distributed sensors converges. As such, it's preferred for the entry generally to own higher energy and process capabilities.

The case of an outsized scale sensing element networks could necessitate the preparation of multiple gateways. Adequate coverage for the world of interest needs placement of the entries within the manner that minimizes inequality between the sizes of the subnet work coated by every gateway.

3.2.1 Random Deployment
Here, we tend to the thought of random deployment of sensors. It means that the node's position within the network isn't thought of antecedently. Random reading of detector nodes within the physical setting might take many forms.

It should be a onetime activity where the installation and use of a detector network are strictly separate actions. Or, it should be endless method, with additional nodes being deployed at any time throughout the utilization of the network; as an example, to exchange failing nodes or to enhance the coverage space at sure locations.

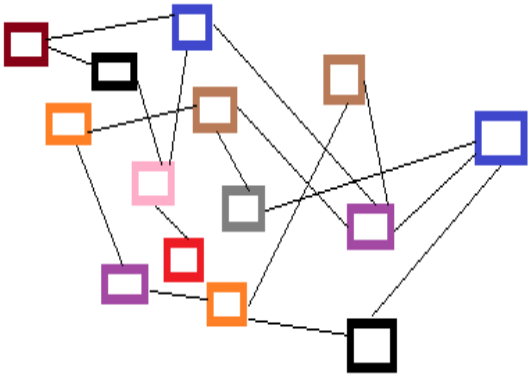

Fig 1: Random Deployment

Figure 1 shows the random deployment of device nodes. The characteristics of random deployment are

- Randomized device deployment has a sort of difficulty in some respects, since there's no need to set up a cloister, the precise location of every device.
- Post deployment self configuration mechanisms are needed to get the required coverage and property.
- In case of an identical random deployment, the sole parameters which will be controlled apriority are the number of nodes and a few connected settings on these nodes, like their transmission parameters.

3.2.2 Grid Deployment
There are basically 3 varieties of grid, primarily based on topology like three regular shapes which might tile a plane, not holes, namely, hexagon, square and trigon. Grid's deployment is primarily conducted by placing sensors row by row employing a moving carrier. The duration between consecutive fatal matters is controlled to realize the required distance.

However, usually this ideal deployment isn't realistic to find the placement errors. In the unreliable detector grid model, n nodes area unit placed on a sq. grid among a unit space, with an explicit chance that a node is active (not failed), and an outlined transmission vary with every node.

- Adding nodes to check wireless network may be a difficult issue, notably once the unit area location constraints within a given setting dictates that wherever nodes can or cannot be placed.
- If the quantity of accessible nodes is less with respect to the scale of the operational space and needed coverage, a balance between sensing and routing nodes needs to be optimized.
- The nodes area unit is typically deployed in not simply accessible areas [6]. Therefore the power needs should be optimized by exploiting appropriate algorithms.

Figure 2 shows the grid sort arrangement of detector nodes wherever the nodes area unit organized in a uniform manner.

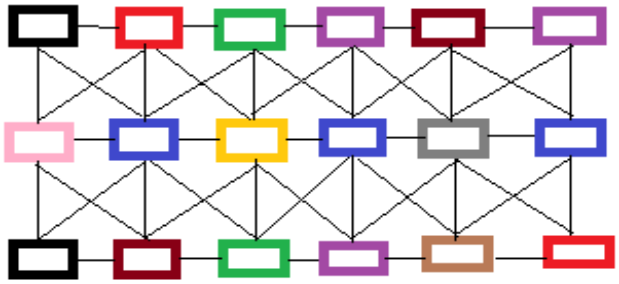

Fig 2: Grid type deployments

3.3 Cluster Formation

In most of the wireless sensor network (WSN) applications, the whole network should have the flexibility to work unattended in harsh environments within which pure human access and observation cannot be simply regular or expeditiously managed or it's even not possible in the slightest degree highlights its crucial expectation [7]. In several important WSN applications the sensor nodes are usually deployed willy-nilly within the space of interest by comparatively unorganized suggestion that forms the network in a poster hoc manner.

A common classification is done between static and dynamic agglomeration. A cluster formation procedure is thought to be dynamic (otherwise as static) once it includes a regular (periodic or event driven) CH election [8] or cluster reorganization procedures [9], either to effectively react to constellation changes and change befittingly the cluster topology, or just aiming at the acceptable rotation of the CH role among the nodes to achieve in energy potency.

Dynamic cluster architectures [10] create a more robust use of the sensors in an exceedingly WSN and naturally result in improved energy consumption management and network life.

Most of the celebrated agglomeration algorithms for WSNs will be additionally distinguished into 2 main classes based on cluster formation criteria and parameters used for CH election

- Probabilistic (random or hybrid) agglomeration algorithms
- Non probabilistic agglomeration algorithms

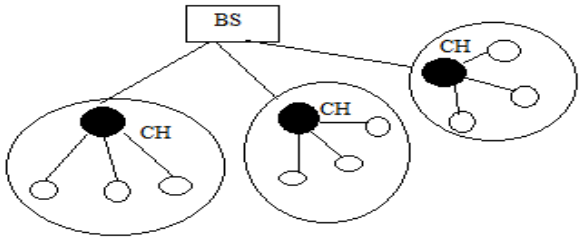

Fig 3: Data communication in clustered network

One among the primary and most well-liked agglomeration protocols [11] projected for WSNs is LEACH (Low Energy Adaptive Clustering Hierarchy) [12]. Figure 3 represents communication in an exceedingly clustered network. The cluster heads are answerable for relaying the info to be transmitted from individual nodes to the bottom station.

Moreover, considering the whole space that must be covered, the short term of the battery, that is the energy of sensors and also the chance of getting broken nodes throughout readying, massive populations of sensing elements are expected; it's a natural chance that lots of or maybe thousands of sensor nodes are going to be concerned [13]. Additionally, sensors in such environments are energy consuming and their batteries sometimes cannot be recharged.

Therefore, it's evident that specialized energy aware routing and information gathering protocols providing high quantifiability ought to be applied so that network period is preserved high in such environments. Naturally, grouping sensing element nodes into clusters has been widely adopted by the analysis of community to satisfy the on top of quantifiability objective and usually to attain high energy potency and to prolong network period in a massive scale WSN environments. The corresponding gradable routing and information gathering protocols imply cluster primarily based on the organization of sensing element nodes so that information fusion and aggregation are attainable, thus resulting in vital energy savings. Within the gradable network structure every cluster features a leader, that is additionally referred to as the cluster head (CH) and typically performs the special tasks [14] referred on top of (fusion and aggregation), and several other common sensing element nodes (SN) as members.

The cluster formation method eventually results in a 2 level hierarchy [15] wherever the CH nodes form the upper level and also the cluster member nodes form the lower level. The sensing element nodes sporadically transmit their information to the corresponding CH nodes. The CH nodes combine the information (thus decreasing the full variety of relayed packets) and transmit them to the base station (BS) either directly or through the intermediate communication with alternative CH nodes. However, since the CH nodes send all the time information to a higher distance than the common (member) nodes, they naturally pay energy at a higher rate.

A common resolution so as to balance the energy consumption among all the network node is to sporadically re elect new CHs (thus rotating the CH role among all the nodes over time) in every cluster [7]. The BS performs the processing purpose of the information received from the sensing element nodes, and wherever the information is accessed by the top user [16]. It is usually mounted at a way distance from the sensing element nodes. The CH nodes really act as a gateway between the sensing element nodes and also the BS. The performance of every CH, is to perform common functions for all the nodes within the cluster, like aggregating the information before passing it to the BS. In a way, the CH is the sink for the cluster nodes, and also the BS is the sink for the CHs.

The transmission of packet in a cluster can be represented using certain algorithms.

Algorithm: DSR blackhole prevention method
Step 1: If node has the data

a. Check route cache
   i. If route is available
      1. Forward the data
   ii. If route is not found
      1. Initiate the route discovery
b. Check the Meli cache

i. If Meli found

1. Update the Meli info in RREQ

Step 2: Broadcast the RREQ

If RREQ received

c. Check the RREQ

i. If Meli_list != Null

1. Update Meli-table

d. Check the Meli Table

i. If forwarder ∈ table

1. Ignore the message

ii. If forwarder ∉Meli table

1. For i∈ Meli table

e. Updates *"i"* in RREQ

i. If current node == destination of the pkt

f. RREQ ⇒RREP

i. Update the reverse route info

ii Send to source

Step 3: If current node ≠destination

b. Broadcast the RREQ as forwarder

Step 4: Meli-maintenance routine

g. If expire time<Current time

i. Delete the Meli ID

Step 5: If RREP is received

h. Check the RREP

i. If Meli_list != Null

1. Update Meli-table

i. Check the Meli Table

i. If forwarder ∈ Meli table

1. Ignore the message

ii. If forwarder ∉Meli table

1. If current node == destination of the pkt

a. Update the reverse route info

b. Send data pkt to destination

i. If current node ≠destination

c. For i∈ Meli table

i. Updates *"i"* in RREP

ii. Forward RREP

3.4 Cluster Head Rotation

There are many other ways to at first distinguish and then to classify the algorithms used for WSNs agglomeration. 2 of the foremost early and customary classifications area unit

- Clustering algorithms for consistent or heterogeneous networks.
- Centralized or distributed agglomeration algorithms.

The first of the on top of classifications is predicted on the characteristics and practicality of the sensors within the cluster, whereas the opposite one is predicted on the strategy that won't belongs to the cluster [8]. In heterogeneous device networks, the area unit is typically composed of 2 styles of sensors, devices with higher processing capabilities and sophisticated hardware (used typically to form some variety of backbone within the WSN being planned because the CH nodes and conjointly function as knowledge collectors and process centers for the knowledge gathered by different sensor nodes), and customary sensors, with lower capabilities, employed to truly sense the specified attributes within the field. In consistent networks, all nodes have a similar characteristics, hardware and process capabilities (this is often the everyday case once the sensors area units are deployed in battle fields).In this case (which is most applicable in the modern applications) each device will become a CH. Moreover, the CH role can be sporadically turned among the nodes so as to bring home the bacon higher load reconciliation and a lot of uniform energy consumption [4].

As they would like for economical use of WSNs on massive regions enhanced within the last decade dramatically, a lot of specific bunch protocols were developed to satisfy the extra necessities (increased network time period, reduced and equally distributed energy consumption, scalability). The foremost important and wide used representatives of those targeted on WSN bunch protocols [11] (LEACH, EEHC, and HEED) [15] and their most precious extensions square measure is bestowed within the main part of this section. They're all probabilistic in nature and their main objective was to scale back the energy consumption and prolong the network time period. A number of them (such as LEACH, EEHC, and related protocols) follow a random approach for CH election (the abs initio allotted possibilities function the idea for the random election of the CHs), whereas others (like HEED and similar approaches) follow a hybrid probabilistic methodology (secondary criteria are thought-about throughout CH election, that's the residual energy).

3.5 Security

Cryptography is that the coding of text in such a fashion that outsider to the code cannot perceive the code, however the specified reader is in a position to decode the cryptography and thus perceive the message.

For early man, even as for contemporary man, there has continuously been a necessity for secrecy, as a result of this sometimes within the interest of each the decoders and encoders [3] that the data not be famed to the final public. In times of war, it's essential that the enemy not apprehend what you and your allies square measure plotting, as a result of winning or losing a war will hinge upon the secrecy of the operations thus to surprise the enemy. However, there was one caveat to any or all the cryptosystems [14] before RSA, that they were all supported by the very fact that each the decrypting and encrypting parties had to understand the tactic of cryptography [2] and also the key [10] to decrypt the cipher.

The goal of security services in WSNs is to guard the data and resources from attacks with minimum computational overhead.

- Availability, that ensures that the specified network services square measure offered even within the presence of denial of service attacks.
- Authorization, that ensures that solely licensed sensors, is concerned in providing info to network services.
- Authentication, that ensures that the communication from one node to a different node is real, that is, a malicious node cannot masquerade as a sure network node.
- Freshness, which means that the info is recent and ensures that no person will replay previous messages. Moreover, as new sensor area unit is deployed and previous sensors fail, we advice that forward and backward secrecy ought to even be thought of.
- Integrity that ensures that a message sent from one node to a different, isn‘t changed by malicious intermediate nodes.
- Non- repudiation, that denotes that a node cannot deny causing a message that is antecedently sent.
- Confidentiality, that ensures that a given message can’t be understood by anyone aside from the specified recipients.

3.5.1 Forward Secrecy

A device shouldn't be able to browse any future messages once it leaves the network.

3.5.2 Backward Secrecy

A change of integrity device shouldn't be able to browse any antecedently transmitted message.

4. RESULTS AND DISCUSSION

In NS2, the code is run in the terminal window. The terminal is like a command prompt in windows. During the running process the two types of files will be generated. One is NAM and another one is Graph. In ensuring secure and efficient data transmission in clustered WSN we use RSA public key encryption algorithm. This is one among the asymmetric algorithms.

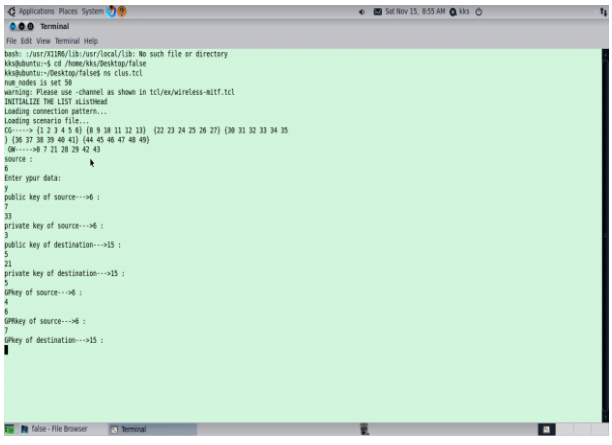

Fig 4: Output terminal 1

The data is encrypted using the source public key and decrypted by the destination private key. This process is used to send the data securely and efficiently.

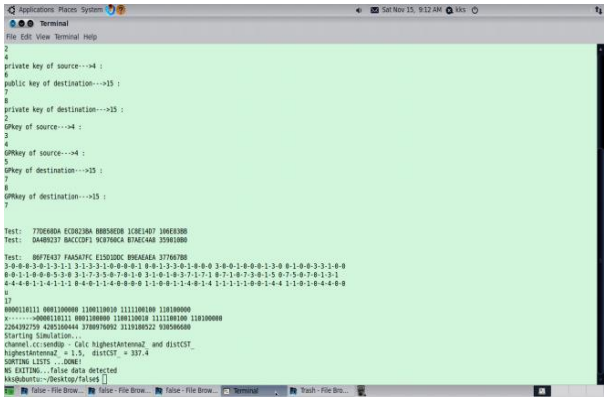

Fig 5 : Output terminal 2

As shown in figure 4, the keys are entered in the output terminal. The source uses 7 and 33 as the public key and the private key is 3. The user defined the destination public key as 5 and 21, the private key is 5. If the keys are wrong the code will returns ‘False Data Detected’.

Figure 5 shows the output terminal where program is run. If the source and destination keys are correct the data will be transmitted to the corresponding destination. In the NAM output, the circles indicate the nodes. Initially all the nodes are in the green color which means all the nodes are in active state.

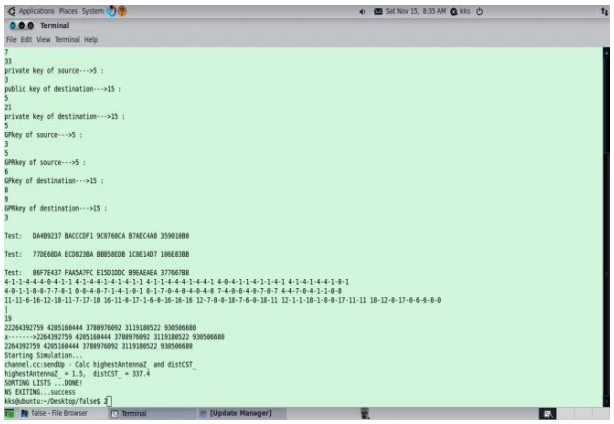

Fig 6: Output terminal 3

After that it has to discover the path to reach the destination. Initially all the nodes are formed in a group called a cluster. In our proposed scheme, we transmit the data in the cluster.

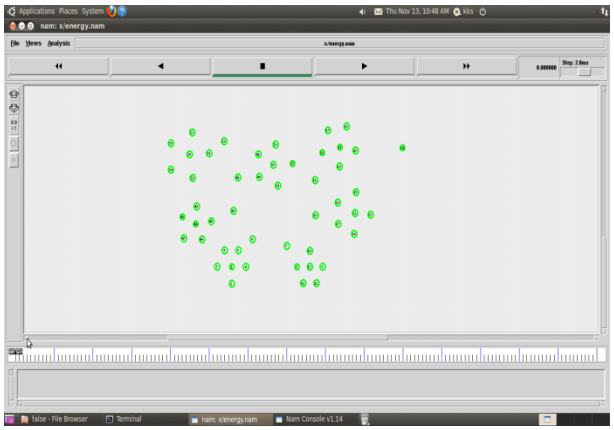

Fig 7: NAM Window 1

In figure 7, the clustered arrangement of node is shown. Each cluster node has a head and a gateway. Inside the cluster the cluster head is used to transfer the data to nodes. Outside the cluster the gateway will help in the data transmission.

For intra cluster communication only cluster heads are involved, while in the case of inter cluster communication, gateways acts as a relay.

Figure 8 shows the discovery process where the nodes need to find the path to transfer to the destination. The discovered nodes are changed as the blue node.

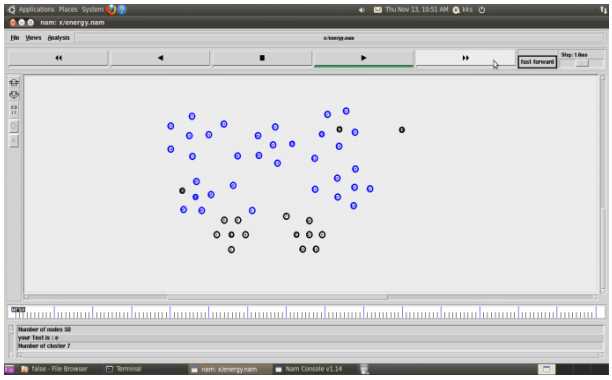

Fig 8: NAM Window 2

Cluster head is indicated in blue color and they are mentioned as CH. The cluster head is also a node, the CH will directly communicate with the gateway node, then identifies the source and destination nodes.

In figure 9, the circles represent the range. During the Discovery process the node forms a circle that is the range of the node and the nodes in the circle are discovered in the process. The hexagonal nodes indicate the CH.

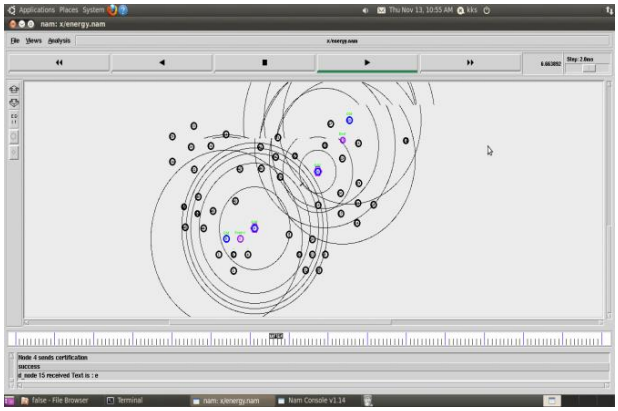

Fig 9: NAM Window 3

The source and destination are indicated by their labels. The source node encrypt the data using source public key and sends to the cluster head(CH), the CH send the data to the Gateway.

The source gateway sends the data to the destination gateway. The destination gateway send the data to the destination CH, the destination CH will send the data to the destination and the destination decrypt the data using his private key.

Most of them, however, apply the symmetric key management for security, which suffers from orphan node problem [16]. This error occurs when a node does not share a pair wise key with others in its preloaded key ring.

Figure 11 shows the graphical analysis based on the overheads of the different protocols used.

To mitigate the storage cost of symmetric keys, the key ring [4] in a node is not enough for it to share pair wise symmetric keys with all of the nodes in a network. In this case, it cannot take part in any cluster, and therefore, has to choose itself as a CH. Also the orphan node problem reduces the possibility of a node joining with a CH, when the number of active nodes owning pair wise keys decreases after a long term operation of the network.

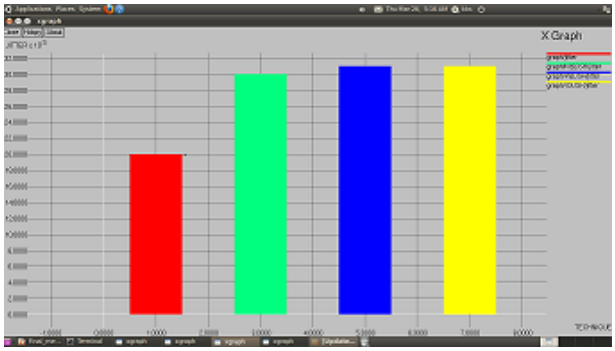

Fig 10: Graphical comparison

The graphical analysis shown in figure 10 gives a comparative study between different routing protocols. The jitter is measured in each case. It is evident that the jitter is less in this proposed scheme. Also an efficient delivery of the packets to the intended destination is ensured.

Since the more CHs elected by themselves, the more overall energy consumed by the network, the orphan node problem increases the overhead of transmission and system energy consumption by raising the number of CHs. Even in this case that a sensor node shares a pair wise key with a distant CH but not a nearby CH, it requires relatively higher energy to transmit data to the distant CH.

Secret keys and pairing parameters are distributed and preloaded in all sensor nodes by the BS initially, which eliminates the key escrow [17] problem.

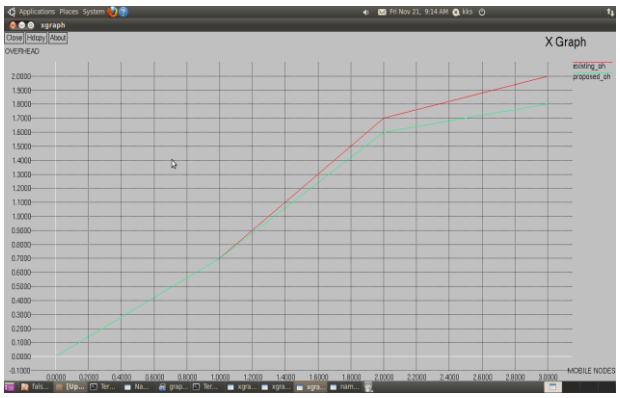

Fig 11: Output graph 1

The graphical analysis in figure 12 shows that the delay is reduced in the case where RSA and HEF algorithm is used.

Digital signature is used for ensuring the security where the binding between the key and identification of user is obtained via a digital certificate which increases the delay and overhead.

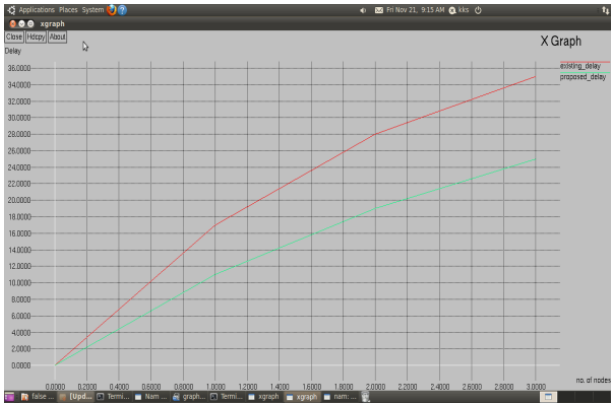

Fig 12: Output graph 2

In this technique, the secret parameters are preloaded at the nodes initially by the base station. This reduces the delay.

It is evident from the figure 13 that the packet delivery fraction is increased in this technique.

As a primary step for efficiency, clustering is done [16]. The cluster head is selected using the High Energy First clustering method which selects the node with highest energy as the cluster head. This increases the network lifetime. Initially the source and the destination nodes for data transmission are chosen and are set for the data transmission. The other nodes are held at the sleep mode which avoids the unwanted energy wastage.

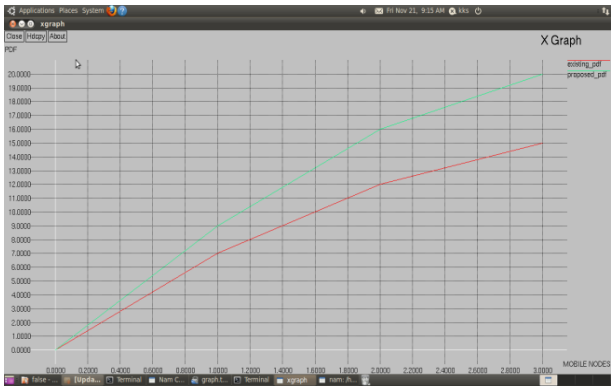

Fig 13: Output graph 3

Table 1. Performance comparison

Protocol	Overhead	Delay	PDF
LEACH, SET IBS	15 %	23 ns	75%
HEF, RSA	7%	16 ns	83%

Table 1 shows the performance comparison between different protocols.

5. CONCLUSION

In this paper, we have first reviewed the information transmission problems and therefore the security problems in CWSNs. We need to transmit our data through a malicious free and wrongdoer free path by trust analysis. The deficiency of the parallel key management for secure knowledge transmission has been mentioned so as to beat the shortcomings of the parallel key management, we have a tendency to use an uneven technique that's RSA algorithmic rule which ensures security with minimum computational overhead. High Energy First cluster technique is employed for selecting the cluster head. The cluster head is chosen based on its energy level. In the analysis section, we have to provide feasibleness of the projected theme with relation to the safety necessities and analysis against routing attacks. This theme is economical in communication and applying the uneven cryptosystem that achieves security necessities in CWSNs, and also solved the orphan node downside within the secure transmission protocols with the parallel key management. It is evident that HEF technique prolongs the network life time by choosing an effective way for the cluster head rotation. Lastly, the comparison within the calculation and simulation results show that the projected technique have higher performance than existing secure protocols for CWSNs. With relation to each security and potency, we have a tendency to detect the phenomena that mistreatment HEF and RSA algorithms with less auxiliary security overhead and is most well-liked for secure knowledge transmission in CWSNs.

6. FUTURE WORK

A framework may be developed that allows sensible development of centralized cluster primarily based protocols supported by improvement ways for the WSNs. Supporting this framework, a protocol victimization harmony search algorithmic rule (HSA), a music primarily based meta heuristic improvement methodology, is meant and enforced in real time for the WSNs. It is expected to attenuate the intra cluster distances between the cluster members and their cluster heads (CHs) and to optimize the energy distribution of the WSN and to match the performance of each existing and planned protocols. The wok can be extended to ensure security in mobile nodes along with the stationary nodes and thereby the scheme gets a wide range of application. The MANETs are usually prone to black hole attacks. Decisions made on the basis of trust calculation method are expected to overcome the shortcomings of OLSR with AODV routing protocol. Clustering is also maintained to keep the overall efficiency high. A comparative study can be performed to find the feasibility of the proposed scheme.

7. REFERENCES

[1] T. Hara, V.I. Zadorozhny, and E. Buchmann,2010 Wireless Sensor Network Technologies for the Information Explosion Era, Studies in Computational Intelligence. vol. 278. Springer-Verlag.

[2] A. Shamir, 1985 Identity-Based Cryptosystems and Signature Schemes, Proc. Advances in Cryptology (CRYPTO), pp. 47-53.

[3] Chris Karlof, David Wagner,2003, Secure routing in wireless sensor networks: attacks and countermeasures, University of California at Berkeley, Berkeley, CA 94720.

[4] D.W. Carman, 2005, New Directions in Sensor Network Key Manage-ment, Int'l J. Distributed Sensor Networks, vol. 1, pp. 3- 15.

[5] F. Hess, 2003,Efficient Identity Based Signature Schemes Based on Pairings, Proc. Ninth Ann. Int'l Workshop Selected Areas in Cryptography (SAC), pp. 310-324.

[6] H. Lu, J. Li, and H. Kameda, 2010. A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks

Using ID-Based Digital Signature, Proc. IEEE GLOBECOM, pp. 1-5.

[7] H Lu, J Li and Mohsen Guizani, 2014. Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Network" IEEE transactions on parallel and distributed systems, vol. 25, no. 3.

[8] J.J. Rotman, 1994. An Introduction to the Theory of Groups, fourth ed. Springer-Verlag.

[9] Joseph K. Liu, Joonsang Baek, Jianying Zhou Yanjiang Yang, 2008. Efficient Online/Offline Identity-Based Signature for Wireless Sensor Network.

[10] Kun Zhang, Cong Wang, 2008. A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management IEEE.

[11] L.B. Oliveira et al., 2007. SecLEACH-On the Security of Clustered Sensor Networks, Signal Processing, vol. 87, pp. 2882-2895.

[12] W. Diffie and M. Hellman, 1976. New Directions in Cryptography, IEEE Trans. Information Theory, vol. IT-22, no. 6, pp. 644654.

[13] A.A. Abbasi and M. Younis, 2007. A Survey on Clustering Algorithms for Wireless Sensor Networks, Computer Comm., vol. 30, nos. 14/15, pp. 2826-2841.

[14] Y Wang, G Attebury,B Ramamurthy,2006, A Survey of Security Issues In Wireless Sensor Networks.

[15] Yongyu Jia, Lian Zhao and Bobby Ma, 2008. A hierarchical clustering-based routing protocol for wireless sensor networks supporting multiple data aggregation qualities, Int. J. Sensor Networks, Vol. 4, Nos. 1/2.

[16] S. Sharma and S.K. Jena, 2011. A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks, Proc. Int'l Conf. Comm., Computing & Security (ICCCS), pp. 146-151.

[17] D. Boneh and M. Franklin, 2001. Identity-Based Encryption from the Weil Pairing, Proc. 21st Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '01), pp. 213-229.