THINK INDIA (Quarterly Journal)

ISSN:0971-1260

Vol-22-Issue-4-October-December-2019

Multicast Data Communication Based On Dynamic Clusteringinwsn Using Diffie-Hellman Algorithm

Ms.C.Suganya, M.Phil Scholar,

PG & Research Department of Computer Science,

Chikkanna Govt. Arts College, Tirupur.

Dr.K.Nandhini, Assistant Professor,

PG & Research Department of Computer Science,

Chikkanna Govt.Arts College, Tirupur.

Abstract: A Wireless Sensor Network (WSN) contains large number of Sensor nodes. Privacy of the user may loss because of unauthorized access of third party. For this issue this paper proposes a Diffie-Hellman Algorithm of public key encryption method to provide more security to the data also here included the multicast method of communication with dynamic node discovery technique to solve the security issues.

Keywords*: Wireless Sensor Network, Security, Sending Message and Multicast Communication.*

I.INTRODUCTION

A Wireless Sensor Network (WSN) contains huge amounts of Sensor nodes. Through the base-station (BS), the sensors nodes were communicating each other in a network. A bigger assortment of sensors licenses for detecting over bigger countries with bigger exactness. Wireless Sensor Networks provide a lot of Sensor nodes that outline the networks for recognition the unfurl of technique and advance learning with respect to the objectives of result back to the end-clients. To exchanging the information, network should give higher correspondence strategy among WSN and will give detecting the node between the networks. In WSN, detecting the node might be a pivotal issue to exchange the information among the nodes [1]. While detecting the node inclusion might be a noteworthy drawback on account of disappointment, power, or commotion precariousness. The significance of this difficulty emerges once a WSN must be set up in inaccessible and commonly unclean space. In those regions, there are a few sections like temperature that must be recorded extremely precisely to evade a blast [2]. Each explosion will build the contamination inside the atmosphere that may be more regrettable in an exceedingly blustery climate. In such zones, a sensor is expected to be sent all over. In any case, there's no assurance that the nodes a consistently disseminated when irregular preparing. the possibility of covering the detecting field while they're not covered and being inside correspondence differ of each choice to be completely associated are diminished [3]..First, we think about the use of existing and proposed security

 Copyright ⓒ 2019Authors

ISSN:0971-1260

Vol-22-Issue-4-October-December-2019

methods for multicast networking, including key dissemination, dynamic key administration, and unwavering quality issues. All through in the paper we provide security strategy using Diffie-Hellman Algorithm in Multicast networks. The Diffie-Hellman key Exchange convention is a cryptographic convention that was created by Whitfield Diffie and Martin Hellman in 1976. The Diffie-Hellman key Exchange algorithm is the accompanying difficulty. Alice and Bob need to share a mystery key for use in a symmetric figure, however their solitary methods for correspondence is uncertain.

II. LITERATURE REVIEW

SwapnaNaik [6] detected data can be sent from various perspectives, before unicast steering was there to a solitary sink node, but because of the wide assortment of WSN applications the nearness of multiple sinks is acknowledged which requires multicast directing for effective information scattering to multiple goals. For any catastrophe reconnaissance or flame dealing with crisis situations different multicast directing protocols have been proposed by numerous analysts. This paper provides an overview of the current multicast directing protocols by exhibiting approach, their preferences and burdens. Further a near investigation of different multicast protocols is done based on various parameters to recognize various issues and moves that should be settled for every last one of them.

P.PrasannLaxmi [7] WSNs discover applications in zones like human services, home robotization, traffic control and so forth. WSN with qualities of self-association, multi-hop, dynamic topology and constrained vitality assets, make it amazingly hard to draw out the lifetime of the network. To drag out the existence time of WSN with restricted vitality assets, Multicast can all the more likely meet the prerequisites of network assets. It has a functioning importance for WSN to expand its execution sooner rather than later. And proposed methodology contrasts the execution of two protocols and ten nodes in each gathering.

L. B. Jivanadham [8] propose an efficient group key management utilizing symmetric key and Threshold Cryptography for Cluster based Wireless Sensor Networks. The proposed plan considers a progressive bunch structure of sensor network and embraces the pair-wise key administration and gathering key administration dependent on limit key cryptography to create and to disseminate the keys effectively inside a group and updates occasionally keys. By thusly EGKMST gives ceaseless transmission security and dodges perilous assaults from noxious nodes and moderate the node bargain assault in WSNs correspondence. The security and execution investigation delineate that EGKMST conspire accomplishes the necessity of gathering correspondence and gives productive security low correspondence cost, low memory overhead and vitality sparing contrasted and some current key administration plans.

.III. METHODOLOGY

The application of wireless sensor networks to areas such as combat field surveillance, terrorist tracking and highway traffic monitoring requires secure communication among the sensor nodes, which under this collaborative model calls for efficient group key management. We analyzed the security and performance of this

 Copyright ⓒ 2019Authors

ISSN:0971-1260

Vol-22-Issue-4-October-December-2019

scheme compared with other ones. Comparison results show that our scheme is low in storage requirement, computational overhead and communication cost.

- The nodes are formulated in groups, where each group member interacts with other group member to forward the processed data from one point to another.
- The process of data aggregation completely fails without multicast communication. Hence, it is very important that a robust security technique is to be developed to address the security issues in group communication system in WSN.

a. Attack Model and Secret Sharing Scheme

The attackers may originate from inside or outside the network. They can listen silently on the traffic infuse new messages, replay and change old messages, or different personalities. As of now referenced above, creator expect the TTP as totally dependable and the NMM as genuine however inquisitive. Creator further accepts that the Network Multicast Manager (NMM) does not work together with malicious nodes. Also, creator expect that the security related data at the nodes and at the NMM is put away in alter safe equipment, which is as of now normal and accessible at a sensible cost.

b. Key Distribution Phase

In the primary stage, the key dispersion stage, the TTP chooses three master secret values*x, y, z F1q*and produces two unique sorts of security related data. The first type is for the node's N_i with $i = 1. . . m$ in the network and the second type is for the NMM. Denote the identity of *Ni* by *IDi* and NMM by ID_{NMM}. For each N_i, the TTP executes the following computations:

$$Ki = H (IDi \,||\, x \,||\, y \,||\, z)$$
$$Ai = H (IDi \,||\, x)$$
$$Bi = H(y) \oplus Ai$$
$$H(Ai) = H (H (IDi \,||\, x))$$

The qualities *Ki, Bi, H(Ai), H(x), IDNMM* are sent over a safe channel (for example by pre-stockpiling) to every node *Ni*. Here, Bi replaces the character of the node for the outside world.

c. Node discovery

 Copyright ⓒ 2019Authors

ISSN:0971-1260

Vol-22-Issue-4-October-December-2019

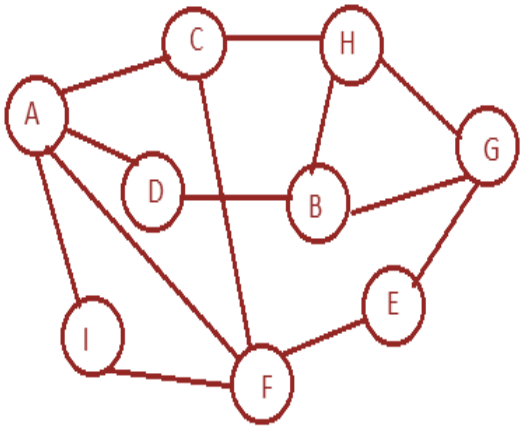


Figure 3.1: Node in WSN

In figure 3.1 all nodes were associated. From this creator need to discover the node which on will give a traffic free and speedy way to convey the bundle to the next node. The node which is halfway to source node will get the RREQ and sets up a turnaround way. This is finished by making the past hop of the solicitation message as the following hop on the switch way. Multiple quantities of RREQ messages came to at a similar node will be disposed of. This will essentially lessen the network burden and postponement in the network. As the RREQ message achieves the goal, a Route Reply (RREP) message is produced and sends back to the source node through a similar way pursued by the RREQ message. The following session is the Route Maintenance. At whatever point the association between any two nodes is harmed or lost, a Route Error (RERR) message is created and sends to all sources through forerunner courses which are kept up discretely. Pre-characterized courses are eradicated by RERR messages in like manner. At the point when a source gets a RERR message, it starts Route Discovery session once more.

d. Multicast Construction Phase

In view of the data got after the enlistment stage, the multicast bunches are made. For each gathering, a multicast address IDG is produced. The NMM communicates the location IDG to every supporter, signified by *Ss, s = 1, . . ., n* (with relating key material *As, Bs)*. To the distributer of the gathering, indicated by P (with comparing key material *Ap, Bp)*, key related data of the supporters in its gathering is sent utilizing their regular shared key *kp*. This key related data for every supporter equivalent to*kps = H(IDGkks)* and is joined with personality *Bs*, for all *Ss* with *s = 1, . . ., n* in the multicast gathering. Therefore, the message *Ekp (B1, kp1... Bn, kpn)* is sent to the distributer. After decoding of this message, P has a typical imparted key to every one of its endorsers.

Copyright ⓒ 2019Authors

ISSN:0971-1260

Vol-22-Issue-4-October-December-2019

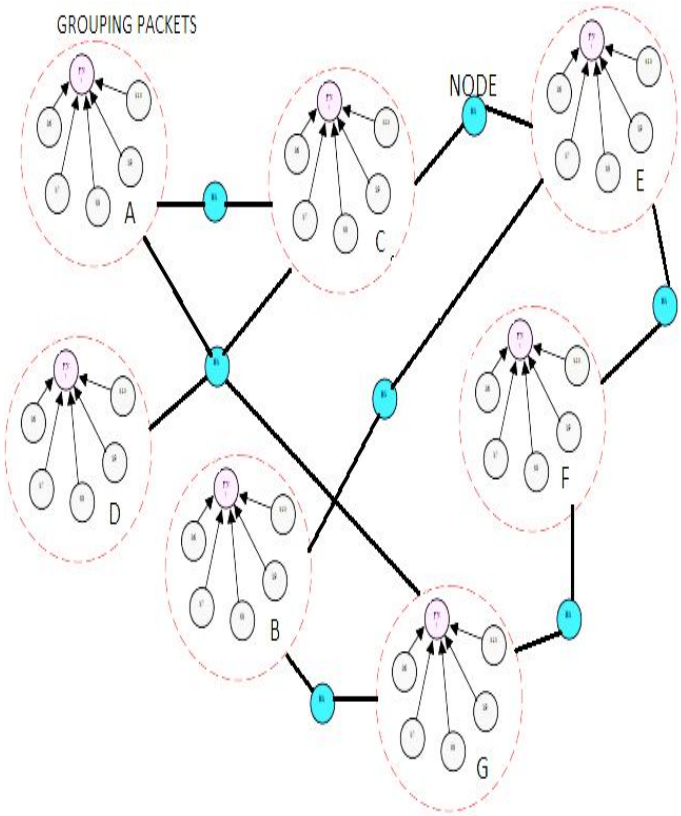


Figure 3.2: Proposed Architecture

Utilizing LI through the n focuses *(xs, ys) = (Bs, kps) with s = 1, . . ., n*, together with the point containing the gathering key *(0, kg)*, a polynomial of degree n can be developed. Next, n different focuses *(v, Vv)* with *v = 1, . . ., n* on this polynomial are inferred. Diffie-Hellman builds up a mutual top mystery that can be utilized for mystery correspondences while trading information on the network. Diffie-Hellman key Exchange is a particular technique for trading cryptographic keys.

IV.RESULTS AND DISCUSSION

4.1 DYNAMIC CLUSTERING DIFFIE - HELLMAN SCHEME

4.1.1 NETWORK MULTICAST MANAGER

Multicast becomes increasingly more important in our everyday lives, effectively managing multicast related interruptions is a primary concern. Users cannot afford to risk continuity of collaboration, information sharing and networking.However, it is necessary to have a vehicle for a postman to carry the packets to be delivered in the destinations. In other words, it is necessary to define multicast routing algorithms in order to deliver internet multicast service.

4.1.2 TRUSTED THIRD PARTY

 Copyright ⓒ 2019Authors

ISSN:0971-1260

Vol-22-Issue-4-October-December-2019

Trusted third party protocol is suffering from both lack of scalability and single point failure. Because the communication entities can achieve mutual authentication and secure communication through the single trusted third- party's assistance. Finally, adopting pre-distribution where the required secret keys are pre-loaded before deploying the nodes has many limitations: it has no immunity against node's capture attack, and it does not enhance the resilience and scalability of the WSN. Actually, the number of stored keys will be increased by increasing the number of deployed nodes. Moreover, if the number of compromised nodes is increased above a specific threshold, then the number of uncompromised nodes will be affected as well.

4.1.3 KEY GENERATION

As the name suggests key pre distribution involves distributing keys to all interested parties before the start of communication. Once deployed, there is no mechanism to include new members in the group or to change the key. In key transport system, one of the communicating entities generates keys and transports them to the other members. It assumes that a shared key is already exists among the participating members. This prior shared key is used to encrypt a new key and is transmitted to all corresponding nodes. Only those nodes which have the prior shared key can decrypt it. Key arbitration schemes use a central arbitrator to create and distribute keys among all participants. Hence, they are a class of key transport schemes. There is a difference in distribution of public keys which belong to a public knowledge, and private (secret) keys which are shared by multiple entities.

4.1.4 KEY REGISTERING

This scheme guarantees that two communicating parties can establish a unique session key between them. Furthermore, it is using key pre-distribution mechanism for a large-scale WSN, based on a hierarchical clustered network model and trusted third party.It takes the advantage of asymmetric cryptographic scheme and pre-distribution mechanism to achieve both key management and authentication. Based on hierarchical clustered model and trusted third party. This section discus the transactions between the involved communicating parties at each layer and their roles, the related keys and their pre-distribution, the three main phases and action during each one, and the adopted asymmetric algorithm for session key generation and authentication of communicating parties.

4.1.5 DISCOVERING THE NODE

Multiple quantities of RREQ messages came to at a similar node will be disposed of. This will essentially lessen the network burden and postponement in the network. As the RREQ message achieves the goal, a Route Reply (RREP) message is produced and sends back to the source node through a similar way pursued by the RREQ message. The following session is the Route Maintenance. At whatever point the association between any two nodes is harmed or lost, a Route Error (RERR) message is created and sends to all sources through forerunner courses which are kept up discretely. Pre-characterized courses are eradicated by RERR messages in like manner. At the point when a source gets a RERR message, it starts Route Discovery session once more.

 Copyright ⓒ 2019Authors

ISSN:0971-1260

Vol-22-Issue-4-October-December-2019

4.1.6 MULTICAST CONSTRUCTION PHASE

In this multicast Constructionphase, these keys are used to send confidential and authenticated messages. IP multicast, applications send one copy of a packet and address it to a group of receivers (at the multicast address) that want to receive it rather than to a single receiver (for example, at a unicast address). In this communication paradigm, a particular device can reach a group of other devices in the network by sending a single message, containing a multicast address. Multicast depends on the network to forward the packets to only those networks and hosts that need to receive them, therefore controlling network traffic and reducing the amount of processing that hosts have to do.

4.6 DIFFIE - HELLMAN BASED SCHEME

It is demonstrated that the Diffie - Hellman based plan is secure up to t disavowed clients. They demonstrate that regardless of whether t clients were not disavowed in polynomial numerous sessions, any endeavour to uncover data on the common mystery at the present session includes the arrangement of an issue that is in any event as hard as DDH.

4.2 PCGR SCHEME

Pre-distribution and local collaboration-based group re-keying protocol (PCGR) this process is to future group keys can be preloaded to the sensor nodes before deployment, and neighbors can collaborate to protect and appropriately use the preloaded keys. The basic idea of the program is: The survival time of sensor networks is divided into a lot of time intervals called the session (sessions).The two group key management scheme are high in security, but there are isolated nodes problem, as well as high computational, storage and communication overhead problem; The design of the scheme is motivated by the following ideas:(1)Secret share which are used to compute the group key are generated by cluster heads, which choose the one-order polynomial to avoid high overhead of computation and storage. (2) The secret shares are encrypted using the secret encryption keys pre-distributed into nodes so that only the legitimate ones can get the secret shares. (3) The generation of group key must need the participation of the random number distributed by cluster heads in order to prevent conspiracy attack.

Analysis proved that our scheme has good security, lower memory overhead and communication overhead.

4.3 COMPARISON DIFFIE - HELLMAN SCHEME AND PCGR

4.3.1 MESSAGE DELAY

 Copyright ⓒ 2019Authors

ISSN:0971-1260

Vol-22-Issue-4-October-December-2019

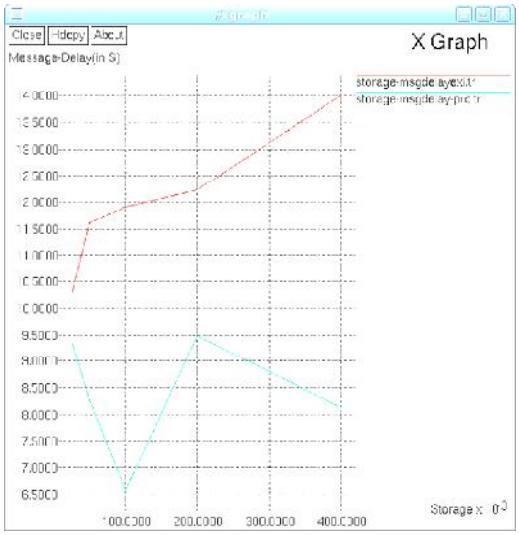


Figure - 1

Figure 1 shows how many messages user will be sent to the networks the messages reach to the destination quickly messages reach the destination in between message sending time will be delay that will be displayed in the above graph.

4.3.2 MESSAGE OVERHEAD

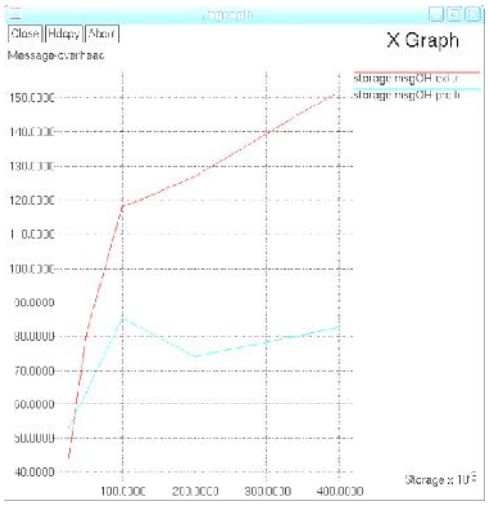


Figure - 2

In figure 3 messages overhead denotes to time and bandwidth. When compared to the existing one our system reduces the bandwidth and time for the message sending in network.

4.3.3 PACKET DELIVERY RATIO

Copyright ⓒ 2019Authors

ISSN:0971-1260

Vol-22-Issue-4-October-December-2019

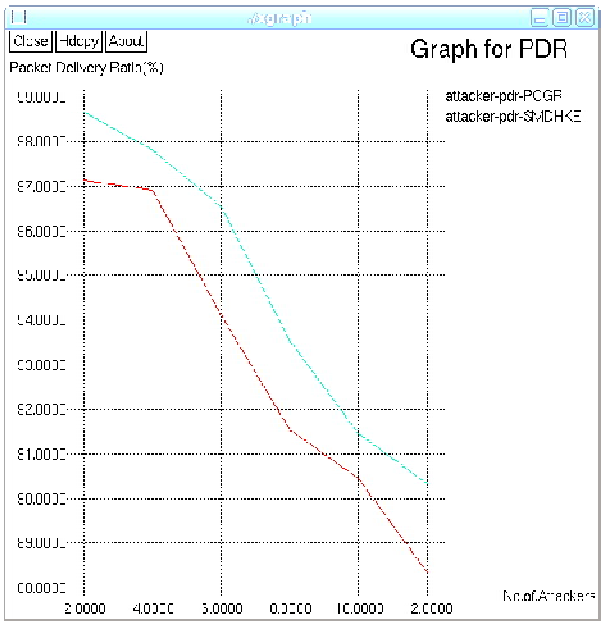


Figure - 3

In this figure 3 it shows the deliver ratio of packets. Our system shows large number of packets was sent without packet loss.

4.3.4 PACKET LOSS

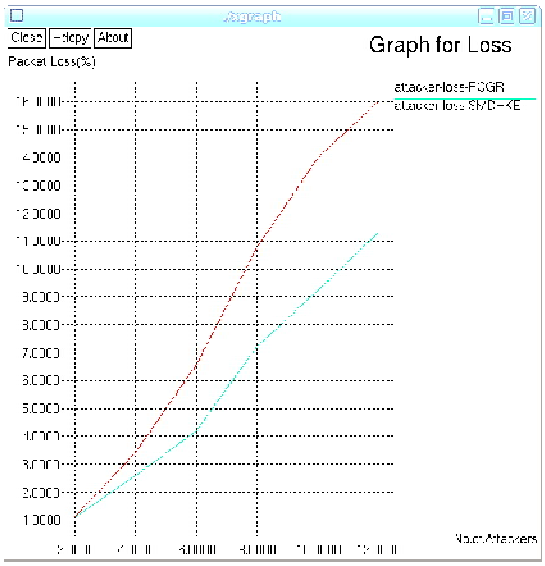


Figure - 4

Packet loss is one of the great issues in network. In figure 4 shows the low-level packet loss. When compared to existing the packet loss was reduced.

V. CONCLUSION

Copyright ⓒ 2019Authors

ISSN:0971-1260

Vol-22-Issue-4-October-December-2019

Many of them, yet, have the limitations of high computational and communication expense in addition to absence of scalability and strength to node compromise problems. To address these issues, we propose Diffie-Hellman key exchange protocol. So, the security of the key distribution and management in wireless sensor networks will get solved by this method.

VI.REFERENCES

[1]. 1.Ahmed, Khandakar, and Mark A. Gregory. "Integrating Wireless Sensor Networks with Cloud Computing." In *MSN*, pp. 364-366. 2011.

[2]. 2.Botta, Alessio, Walter De Donato, Valerio Persico, and Antonio Pescapé. "On the integration of cloud computing and internet of things." In *2014 International Conference on Future Internet of Things and Cloud*, pp. 23-30. IEEE, 2014.

[3]. 3.Subashini, Subashini, and VeerarunaKavitha. "A survey on security issues in service delivery models of cloud computing." *Journal of network and computer applications* 34, no. 1 (2011): 1-11.

[4]. 4.Takabi, Hassan, James BD Joshi, and Gail-JoonAhn. "Security and privacy challenges in cloud computing environments." *IEEE Security & Privacy* 8, no. 6 (2010): 24-31.

[5]. 5.Wang, Cong, Qian Wang, KuiRen, and Wenjing Lou. "Privacy-preserving public auditing for data storage security in cloud computing." In *2010 proceedings ieeeinfocom*, pp. 1-9. Ieee, 2010.

 Copyright ⓒ 2019Authors