IJRSET NOVEMBER 2016 Volume 3, Issue 11 Pages: 44-55

ISSN 2394-739X

International Journal for Research in Science Engineering and Technology

DESIGNING A CLUSTER SCHEMEOF DSR ROUTING MECHANISM USING RANDOM KEY PRE-DISTRIBUTION IN MANET

[1] N. Umadevi, [2] M. Manoj Kumar,
[1] Head of the Department, [2] M.Phil Research Scholar,
[1] Department of Computer Science and Information Technology, [2] Department of Computer Science,
[1, 2] Sri Jayendra Saraswathy Maha Vidyalaya College of Arts and Science,
[1, 2] Coimbatore, Tamil Nadu, India.

ABSTRACT: Innovative techniques that improve energy efficiency to prolong the network lifetime are highly required. Clustering is an effective topology control approach in wireless sensor networks, which can increase network scalability and lifetime. In this paper, we propose a novel clustering schema for wireless sensor networks, which better suits the periodical data gathering applications. Our approach elects cluster heads with more residual energy through local radio communication while achieving well cluster head distribution. And this scheme is secure against adaptive chosen-message attacks. Preventing or detecting malicious nodes launching gray hole or collaborative black hole attacks is a challenge. This paper attempts to resolve this issue by designing a dynamic source routing (DSR)-based routing mechanism, which is referred to as the RKP (Random Key Pre-distribution) that integrates the advantages of both proactive and reactive defense architectures. Our RKP method implements a reverse tracing technique to help in achieving the stated goal.

KEYWORDS: [Ad Hoc Network (MANET), cluster, DSR, RKP.]

1. INTRODUCTION

As the wireless network technology exploded, it has opened a new view to users and expanded the information and application sharing very conveniently and fast. Mobile ad hoc networks (MANETs) use wireless technology without a pre-existing infrastructure (access points). As the name states, MANETs consists of mobile nodes, which can vary from notebooks, PDAs to any electronic device that has the wireless RF transceiver and message handling capability. Mobility and no-infrastructure forms the basis of this network type. Mobility gives maximum freedom to users, as they can be connected to the network, whether they are fixed or moving, unless they are in the range of the network. Also, it is highly dynamic, as the new nodes come, they can be connected to the network very easily. Unlike the fixed networks or traditional wireless networks, MANETs don't need any infrastructure to create and maintain communication between nodes. This property provides the ability to create a network in very unexpected and urgent situations very quickly, also without any extra cost.

Figure1- Mobile Ad hoc Network

2. STRUCTURE OF AD HOC NETWORKS

As we said any electronic device that has the wireless transmission capability with proper processing hardware can be a part of a MANET. So, firstly the nodes have to have RF wireless transceivers as the network interface. But since the wireless transmission ranges according to transmission type of the antenna (omni drectional, bidirectional), and the variations between transceivers at different nodes effect the network structure of the MANETs. However, members of the MANETs can be fixed without any constraint, they consist of mobile nodes. So, their processing capability is limited. Also, power consumption of the mobile nodes is a very great factor on the structure of the MANETs. So, to make MANETs applicable and get maximum performance from them, we have to consider these two factors, and design any algorithms appropriately. MANETs are autonomous and decentralized networks. So, they can operate no matter which nodes are connected or not connected to the network. Connectivity of nodes only affects the topology and routing of the network, not the general operations. Since, MANETs don't have any centralization; operations are done distributed, so each node has to have sufficient information about the network and have to operate independently. Two nodes that want to communicate with each other can send and receive messages directly, if they are both in their transmission range. Otherwise, every node is also capable to be a router, and the messages between nodes are relayed by the intermediate nodes, from the originator of the message to the destination. Since the nodes are mobile and the members of the network changes without any notice, the network structure is very dynamic. So, the route the messages are sent by, are dynamic also. Routing is a very vital and performance critic issue for ad hoc networks. So, we are going to handle that procedure in deep.

3. LITERATURE REVIEW CBDS:

3.1 A COOPERATIVE BAIT DETECTION SCHEME TO PREVENT MALICIOUS NODE FOR MANET BASED ON HYBRID DEFENSE ARCHITECTURE

With the widespread use of mobile devices, the users of Mobile Ad hoc network (MANET) become increasingly more, which results the rapid development of the technology. Due to MANET don't need the infrastructure, it can deploy fast and conveniently in any environment. Because of its easy deployment features, in addition to used in personal area networks, home area networks and so on. Specially, MANET suit for military operations and the emergent disasters rescue that need to overcome terrain and special purpose in urgent. However the dynamical network topology of MANET, infrastructure-less property and lack of certificate authority make the security problems of MANET need to pay more attention.The common routing protocols in current such as DSR AODV and so on almost take account in performance. They don't have the related mechanism about detection and response. Aiming at the possible attacks by malicious nodes, based on the DSR protocol, this paper presented a mechanism to detect malicious nodes launching black/gray hole attacks and cooperative black hole attacks, known as Cooperative Bait Detection Scheme (CBDS). It integrates the proactive and reactive defense architectures, and randomly cooperates with a stochastic adjacent node. By using the address of the adjacent node as the bait destination address, it baits malicious

nodes to reply RREP and detects the malicious nodes by the proposed reverse tracing program and consequently prevents their attacks.

3.1.1 MOBILE AD HOC NETWORKING (MANET)

Routing Protocol Performance Issues and Evaluation Considerations With recent performance advancements in computer and wireless communications technologies, advanced mobile wireless computing is expected to see increasingly widespread use and application, much of which will involve the use of the Internet Protocol (IP) suite. The vision of mobile ad hoc networking is to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes. Such networks are envisioned to have dynamic, sometimes rapidly-changing, random, multi-hop topologies which are likely composed of relatively bandwidth-constrained wireless links. Within the Internet community, routing support for mobile hosts is presently being formulated as "mobile IP" technology. This is a technology to support nomadic host "roaming", where a roaming host may be connected through various means to the Internet other than its well known fixed-address domain space. The host may be directly physically connected to the fixed network on a foreign subnet, or be connected via a wireless link, dial-up line, etc. Supporting this form of host mobility (or nomad city) requires address management, protocol interoperability enhancements and the like, but core network functions such as hop-by-hop routing still presently rely upon pre- existing routing protocols operating within the fixed network. In contrast, the goal of mobile ad hoc networking is to extend mobility into the realm of autonomous, mobile, wireless domains, where a set of nodes--which may be combined routers and host- themselves forms the network routing infrastructure in an ad hoc fashion.

3.1.2 AN EFFICIENTMESH-BASED CORE MULTICAST ROUTING PROTOCOL ON MANETS

Mesh-based multicast routing protocols for mobile ad hoc networks (MANETs) build multiple paths from senders to receivers to deliver packets even in the presence of links breaking. This redundancy results in high reliability/robustness but may significantly increase packet overhead. This paper proposes a mesh-based multicast protocol, called centered protocol for unified multicasting through announcements (CPUMA), that achieves comparable reliability as existing mesh-based multicast protocols, however, with significantly much less data overhead. In CPUMA, a distributed core-selection and maintenance algorithm is used to find the source-centric center of a shared mesh. We leverage data packets to center the core of each multicast group shared mesh instead of using GPS or any pre-assignment of cores to groups (the case of existing protocols). The proposed centering scheme allows reducing data packet overhead and creating forwarding paths toward the nearest mesh member instead of the core to reduce latency. We show, via simulations, that CPUMA outperforms existing multicast protocols in terms of data packet overhead, and latency while maintaining a constant or better packet delivery ratio, at the cost of a small increase in control overhead in a few scenarios.

3.1.3 TBONE: A MOBILE-BACKBONE PROTOCOL FOR AD HOC WIRELESS NETWORKS

We introduce an ad hoc wireless mobile network that employs a hierarchical networking architecture. The network uses high capacity and IOU, capacity nodes. We present a topological synthesis algorithm that selects a subset of high capacity nodes to form a backbone network. The latter consists of interconnected backbone nodes that intercommunicate across high power links, and also makes use of (air home, ground and underwater) Unmanned Vehicles (UVs). Each

backbone node manages the allocation of communications resources for transport of messages frond to itself and among nodes that reside in its managed cluster of nodes (access net). Backbone nodes also interact to coordinate the allocation of MAC layer communications sets (such a? time slots) in their access nets to prevent (cross net) interferences. When covered by a backbone node, a mobile node is granted a proper set of time slots (or, equivalently, YDMA andior COMA slots) for direct communications to a local destination, or for accessing the dynamically long-range communications. When uncovered, a node uses a flat multi-hop ad hoc networking scheme. We introduce the TBONE protocol to implement the key networking schemes for such a Mobile Backbone Network (MBN). It includes combined network layer operation, i.e. mobile backbone network topological synthesis, and MAC layer resource allocation schemes. The TBONE protocol serves lo allocate resources across the network to ensure that user applications are granted acceptable quality-of-service (QoS) performance, while striving to ensure a highly ,survivable and robust backhone oriented networking architecture. We present elements of the protocol and key involved algorithms, and illustrate the distinctive advantages offered by the TBONE based mobile backbone network.

3.1.4. AVOIDING BLACKHOLE AND COOPERATIVEBLACKHOLE ATTACKS IN WIRELESS AD HOC NETWORKS

In wireless ad hoc networks, the absence of any control on packets forwarding, make these networks vulnerable by various deny of service attacks (DoS). A node, in wireless ad hoc network, counts always on intermediate nodes to send these packets to a given destination node. An intermediate node, which takes part in packets forwarding, may behave maliciously and drop packets which goes through it, instead of forwarding them to the following node. Such behavior is called black hole attack. In this paper, after having specified the black hole attack, a secure mechanism, which consists in checking the good forwarding of packets by an intermediate node, was proposed. The proposed solution avoids the black hole and the cooperative black hole attacks. Evaluation metrics were considered in simulation to show the effectiveness of the suggested solution. Ad hoc network security is a serious problem by which researchers were concerned. Several security solutions are suggested but perfect security is far from beings obvious. We focused in this paper to the black hole attack, which refuses to convey the traffic and drop it. After the black hole attack specification in an example of routing protocol (AODV), we proposed a solution, based on the principle of Merkle tree, for avoiding the black hole and the cooperative black hole attacks.

3.1.5 MITIGATING ROUTING MISBEHAVIOR IN MOBILE AD HOC NETWORKS

This paper describes two techniques that improve throughput in an ad hoc network in the presence of nodes that agree put in an ad hoc network in the presence of nodes that agree to forward packets but fail to do so. To mitigate this problem, we propose categorizing nodes based upon their dynamically measured behavior. We use a watchdog that identifies misbehaving nodes and a patl~rater that helps routing protocols avoid these nodes. Through simulation we evaluate watchdog and pathrater using packet throughput, percentage of overhead (routing) transmissions, and the accuracy of misbehaving node detection. When used together in a network with moderate mobility, the two techniques increase throughput by 17% in the presence of 40% misbehaving nodes, while increasing the percentage of overhead transmissions from the standard routing protocol's 9% to 17%. During extreme mobility, watchdog and pathrater can increase network throughput by 27%, while increasing the overhead transmissions from the standard routing protocol's 12% to 24%. 1. derlying routing algorithm. We introduce two

extensions to the Dynamic Source Routing algorithm (DSR) [12] to mitigate the effects of routing misbehavior: the watchdog and the pathratcr. The watchdog identifies misbehaving nodes, while the pathrater avoids routing packets through these nodes. When a node forwards a packet, the node's watchdog verifies that the next node in the path also forwards the packet. The watchdog does this by listening promiscuously to the next node's transmissions. If the next node does not forward the packet, then it is misbehaving. The pathrater uses this knowledge of misbehaving nodes to choose the network path that is most likely to deliver packets.

3.1.6 AN ACKNOWLEDGEMENT BASED APPROACH FOR THE DETECTION OF ROUTING MISBEHAVIOR IN MANETS

This paper presents the results of studies under taken routing misbehavior in MANETs (Mobile Ad Hoc Networks). The node misbehaviors may be introduced, due to the open structure and scarcely available battery-based energy, and such routing misbehavior is caused by the selfish nodes that when processor participate in the route discovery and maintenance refuses to forward the data packets. In the present studies it is proposed a novel scheme named 2ACK which provides an add-on technique for routing schemes that detects the routing misbehavior and to overcomes their adverse effect. The main feature of 2ACK is to send two-hop acknowledgment packets in the opposite direction of the routing path and to reduce additional routing overhead. The performances of the proposed scheme were analyzed and simulated and 95% packet delivery ratios were achieved when 40% misbehaving nodes were present in the MANETs. The basic features of the present proposed 2ACK scheme are as follows. when a node forwards a data packet successfully over the next hop, the destination node of the next-hop link sends back a special two-hop acknowledgment called as 2ACK indicating the successful data packet transmission. The 2ACK transmission takes place only for the fraction of data packets, but not for all. Such a selective acknowledgment reduces the additional routing overhead.

4. CLUSTERING SCHEME OF RANDOM KEY PRE-DISTRIBUTION USING DSR PROTOCOL

The frame work, use hybrid techniques are clustering scheme and RKP for improve network life time and security In this paper, we propose and evaluate an energy efficient clustering scheme for periodical data gathering applications in WSNs. In the cluster head election phase, a constant number of candidate nodes are elected and compete for cluster heads according to the node residual energy. The competition process is localized and without iteration, thus it has much lower message overhead. The method also produces a near uniform distribution of cluster heads. And this cooperation is a cost-intensive activity and some nodes can refuse to cooperate, leading to a selfish node behavior. Many message authentication schemes have been developed, based on either symmetric-key cryptosystems or public-key cryptosystems. In our proposed using RKP (Random Key Pre-distribution) .RKP schemes have several variants. Their system works by distributing a key ring to each participating node in the sensor network before deployment. We propose a key management scheme that relies on probabilistic key sharing among nodes within the sensor network. In WSN, the clustering protocol is a key factor in achieving energy efficiency, so the design of an energy-efficient clustering protocol for WSN is very important. In WSNs the sensor nodes are energy constrained. Therefore, it is very important to find some solutions to offer high scalability and satisfy high energy efficiency to prolong network lifetime. One solution is by grouping sensor nodes into sets called clusters. Clustering achieves better lifetime of the sensor network by breaking the sensor network into groups of sensors to

conserve communication energy. As a result, saving the energy and increasing the overall lifetime of the network is achieved. Adopting clustering scheme produces two-level hierarchy; the higher level and the lower level. The higher level is formed by the nodes that are responsible for aggregating and fusing the received data from sensor nodes in the sensing area and then transmit it to a central processor; such nodes are called the Cluster Head (CH) nodes. The lower level of the hierarchy is formed by the nodes that are responsible for detecting the required data from the sensing region and then sending it to the corresponding CH. Each cluster includes number of sensor nodes and one cluster head (CH). CH selection can be centralized performed by the BS or the end user based on some criterion. It can also be distributed in nature and performed by the sensors themselves on a localized level. The BS is responsible for processing data received from sensor nodes to be used by the end user. we propose a novel distributed energy efficient cluster head selection algorithm in which two factors are incorporated: the sensors' residual energy levels and the distances between sensors and the CH.In this process the framework of random key pre-distribution to address the bootstrapping problem. First, we propose the random key pre-distribution scheme, which achieves greatly strengthened security under small scale attack while trading off increased vulnerability in the face of a large scale physical attack on network nodes. We will explain why this trade-off is a desirable one. Second, we present the multi-path key reinforcement scheme, which substantially increases the security of key setup such that an attacker has to compromise many more nodes to achieve a high probability of compromising any given communication. Finally, we propose the random-pair-wise keys scheme, which assures that, even when some number of nodes have been compromised, the remainder of the network remains fully secure. Furthermore, this scheme enables node-to-node mutual authentication between neighbors and quorum-based node revocation without involving a base station. Node-to-node mutual authentication here refers to the property that any node can ascertain the identity of the nodes that it is communicating with. To the best of our knowledge, no previous security scheme for sensor networks supports efficient node-to-node authentication without involving a base station.

4.1 DSR PROTOCOL

The DSR protocol is composed of two mechanisms that work together to allow the discovery and maintenance of source routes in the ad hoc network: Route Discovery is the mechanism by which a node S wishing to send a packet to a destination node D obtains a source route to D. Route Discovery is used only when S attempts to send a packet to D and does not already know a route to D. 3 Route Maintenance is the mechanism by which node S is able to detect, while using a source route to D, if the network topology has changed such that it can no longer use its route to D because a link along the route no longer works. When Route Maintenance indicates a source route is broken, S can attempt to use any other route it happens to know to D, or can invoke Route Discovery again to find a new route. Route Maintenance is used only when S is actually sending packets to D.Route Discovery and Route Maintenance each operate entirely on demand. In particular, unlike other protocols, DSR requires no periodic packets of any kind at any level within the network. For example, DSR does not use any periodic routing advertisement, link status sensing, or neighbor detection packets, and does not rely on these functions from any underlying protocols in the network. This entirely on-demand behavior and lack of periodic activity allows the number of overhead packets caused by DSR to scale all the way down to zero, when all nodes are approximately stationary with respect to each other and all routes needed for current communication have already been discovered. As nodes begin to move more or as communication patterns change, the routing

packet overhead of DSR automatically scales to only that needed to track the routes currently in use. In response to a single Route Discovery (as well as through routing information from other packets overheard), a node may learn and cache multiple routes to any destination. This allows the reaction to routing changes to be much more rapid, since a node with multiple routes to a destination can try another cached route if the one it has been using should fail. This caching of multiple routes also avoids the overhead of needing to perform a new Route Discovery each time a route in use breaks. The operation of Route Discovery and Route Maintenance in DSR are designed to allow uni-directional links and asymmetric routes to be easily supported. In particular, as noted in Section 2, in wireless networks, it is possible that a link between two nodes may not work equally well in both directions, due to differing antenna or propagation patterns or sources of interference. DSR allows such uni-directional links to be used when necessary, improving overall performance and network connectivity in the system. DSR also supports internetworking between different types of wireless networks, allowing a source route to be composed of hops over a combination of any types of networks available [Broch 1999b]. For example, some nodes in the ad hoc network may have only short-range radios, while other nodes have both short-range and long-range radios; the combination of these nodes together can be considered by DSR as a single ad hoc network. In addition, the routing of DSR has been integrated into standard Internet routing, where a “gateway” node connected to the Internet also participates in the ad hoc network routing protocols; and has been integrated into Mobile IP routing, where such a gateway node also serves the role of a Mobile IP foreign agent.

4.2 CLUSTERING SCHEME

Clustering is a useful technique for reducing energy consumption in wireless sensor networks (WSN). To achieve a better network lifetime performance, different clustering algorithms use various parameters for cluster head (CH) selection. For example, the sensor's own residual energy as well as the network's total residual energy are used. In this paper, we propose an energy aware clustering that incorporates both the residual energy levels of sensors within a cluster radius as well as the distances. To achieve this, we define a metric that is calculated at each sensor based on local information within its neighborhood. This metric is incorporated within the CH selection probability. Using this metric, one can choose the sensors with low residual energy levels to have the greatest impact on CH selection which results in CH selection being biased to be close to these sensors. This results in reducing their communication energy cost to the CH.In this process, the clustering protocol is a key factor in achieving energy efficiency, so the design of an energy-efficient clustering protocol for WSN is very important. In WSNs the sensor nodes are energy constrained. Therefore, it is very important to find some solutions to offer high scalability and satisfy high energy efficiency to prolong network lifetime. One solution solution is by grouping sensor nodes into sets called clusters. Clustering achieves better lifetime of the sensor network by breaking the sensor network into groups of sensors to conserve communication energy. As a result, saving the energy and increasing the overall lifetime of the network is achieved. Adopting clustering scheme produces two-level hierarchy; the higher level and the lower level. The higher level is formed by the nodes that are responsible for aggregating and fusing the received data from sensor nodes in the sensing area and then transmit it to a central processor; such nodes are called the Cluster Head (CH) nodes. The lower level of the hierarchy is formed by the nodes that are responsible for detecting the required data from the sensing region and then sending it to the corresponding CH. Each cluster includes number of sensor nodes and one cluster head (CH). CH selection can be centralized performed by the BS or the end user based on some criterion. It can also be distributed in

nature and performed by the sensors themselves on a localized level. The BS is responsible for processing data received from sensor nodes to be used by the end user. In this paper, we propose a novel distributed energy efficient cluster head selection algorithm in which two factors are incorporated: the sensors' residual energy levels and the distances between sensors and the CH.

Process steps:

For ; : maximum number of rounds
For , is the index for sensor node
Find set(sensors in cluster radius)
Calculate weight
Calculate cluster weight
Perform CH selection
Inform all sensor nodes in the cluster
Cluster formation will begin
End of current round condition
Restart new round condition

In network the sensor nodes are often grouped into individual disjoint sets called a cluster, clustering is used in WSNs, as it provides network scalability, resource sharing and efficient use of constrained resources that gives network topology stability and energy saving attributes. Clustering schemes offer reduced communication overheads, and efficient resource allocations thus decreasing the overall energy consumption and reducing the interferences among sensor nodes. A large number of clusters will congest the area with small size clusters and a very small number of clusters will exhaust the cluster head with large amount of messages transmitted from cluster members. Proposed protocol is hierarchical routing based on clustering and find the optimal number of clusters in WSNs in order to save energy and enhance network lifetime. In this work, we have surveyed the state-of-art of clustering algorithms in WSNs.

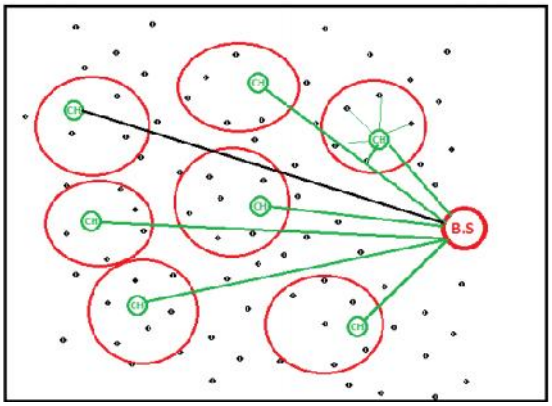


Figure 2- Clustring Scheme

5. RANDOM KEY PRE DISTRIBUTION

Generally, a key establishment scheme has nothing to do with the routing protocol. However, the path in lots of RKPD schemes, such as the basic scheme, is set up through a routing protocol. That is, a customized routing protocol needs to be used along with those key distribution schemes, which will seriously affect the portability of those RKPD schemes. Moreover, the number of hops of the path may increase because the adjacent nodes in the path must be logically connected. In fact, the total amount of computation cost for deciding whether a shared key exists in key rings of two adjacent nodes is also very huge because the routing process may involve many nodes. The basic steps of Phase 3 are changed, and a path that the adjacent nodes only need to be physically connected can be achieved by original routing protocols. To reduce the communication overload, a seed-based method is used to choose key ring for each node upon the input of node's identifier. Although the seed-based method has been mentioned, we firstly construct a deterministic algorithm, with which the times that each key is selected by nodes approximate the average value. In addition, the connectivity of the new scheme is also higher if suitable parameters are chosen. Specifically, when the number of neighbors is less than the predefined out-degree due to the node dormancy or death, the probability that the entire network is connected still approaches 1 by setting a small

amount of redundancy in parameters. The probability that a link is compromised when nodes are captured in our scheme is equal to that of the basic scheme, and it is higher than that of the -composite scheme and that of the -path scheme. However, the probability that a path key is compromised in the establishment phase is lower than that of -path schemes when the number of hops is more than. Our scheme is less competitive in terms of the computation and communication complexity analysis. However, the execution time of a path key establishment for our scheme is slightly less than that of the basic scheme in the simulation. The reason is that, the complexity does not include the extra traffic and calculations that are caused by the customized routing protocol in the basic scheme.

6. PROPOSED METHODOLOGY OF CLUSTER FORMATION

The nodes energy is the most important issue because the nodes are small in size thus making battery replacement unpractical and impossible. Therefore, it is more practical to save energy and prolong the network lifetime by improving the routing algorithm. Cluster based hierarchical routing protocol is an energy efficient routing protocol. In the cluster routing, the sensor nodes will be divided into a few groups with one cluster head elected for each group. The cluster head collects data from member nodes in the same cluster and aggregates the collected data so that it can be transmitted to the base station. Routing techniques are the most important issues for such kind of network where resources are limited. Cluster-base organization has been proposed to provide an efficient way to save energy during communication. In this kind of organization, nodes are organized into clusters. Cluster heads (CHs) pass messages between groups of nodes (group for each CH) and the base station (BS). This organization provides some energy saving, and that was the main idea for proposing this organization. Depending on this organization, protocol added another interesting issue to this kind of network, security, where the CHs are rotating from node to node in the network making it harder for intruders to know the routing elements and attack them.In this phase, several cluster heads are elected. Nodes become CANDIDATE nodes with a probability T and then broadcast the COMPETE HEAD MSGs within radio range R compete to advertise their wills. Each CANDIDATE node checks whether there is a CANDIDATE node with more residual energy within the radius R compete. Once the CANDIDATE node finds a more powerful CANDIDATE node, it will give up the competition without receiving sub sequential COMPETE HEAD MSGs. Otherwise, it will be elected as HEAD in the end.It is necessary to propose a metric that quantifies how good a sensor node could be as a CH. This metric needs to take into account both the residualenergy of sensor nodes in addition to the energy expenditure in transmitting data in intra-cluster communication. As noted from energy model, the energy expended in intra-cluster communication is proportional with distance, therefore it is preferred for a CH to be as close as possible to the sensor nodes in its cluster radius. Moreover, sensor nodes with a low residual energy should have more impact in the CH selection process. Sensors are deployed randomly in a square region. The model has n sensor nodes, which are deployed randomly in a 100 × 100 square meters region as displayed in Figure 1. Base station is located in middle of the sensing region and the distance of any node to its cluster head or sink is ≤ d0. The energy dissipated in the cluster head in a single round is given by Equation.

$$E_{CH} = \left(\frac{n}{k} - 1\right) \times L \cdot E_{elec} + \frac{n}{k} L \cdot E_{DA} + L \cdot E_{elec} + L \cdot \varepsilon_{fs} \cdot d_{toBS}^2$$

Where L is the no of bits of the message, d to BS is the average distance between the base station and cluster head and EDA is the energy required for performing data fusion or aggregation in a round. Since cluster members, send data to its cluster head therefore energy consumed in a non cluster

head follows the free space path and it is given by Equation.

$$E_{NCH} = L \times (E_{elec} + \varepsilon_{fs} \times d^2_{toCH})$$

6.1 SET PROTOCOL

In this module, Secure and Efficient data Transmission protocol for CWSNs. The protocol is designed with the same purpose and scenarios for CWSNs with higher efficiency. The proposed scheme operates similarly to the previous Key management, which has a protocol initialization prior to the network deployment and operates in rounds during communication. first introduce the protocol initialization, then describe the key management of the protocol by using the scheme, and the protocol operations afterwards. This method used for secure access and data transmission to nearby sensor nodes, by authenticating with each other. The probability of neighborhood authentication, where only the nodes with the pair wise key can authenticate each other.

6.2 KEY MANAGEMENT FOR SECURITY

In this module, security is based on the multiplicative group. The corresponding private pairing parameters are preloaded in the sensor nodes during the protocol initialization. In this Module, the key cryptographies used in the protocol to achieve secure data transmission, which consist of symmetric and asymmetric key based security. This scheme enables the intermediate nodes to authenticate the message so that all corrupted message can be detected and dropped to conserve the sensor power. It proposed an efficient key management framework to ensure isolation of the compromised nodes.

Key management deals with the secure generation, distribution, and storage of keys. It plays a vital role in computer security today as practical attacks on public-key systems are typically aimed at key management as opposed to the cryptographic algorithms themselves. This report will investigate the techniques used in the distribution of secret keys used to decrypt and encrypt messages with particular focus key distribution scheme.

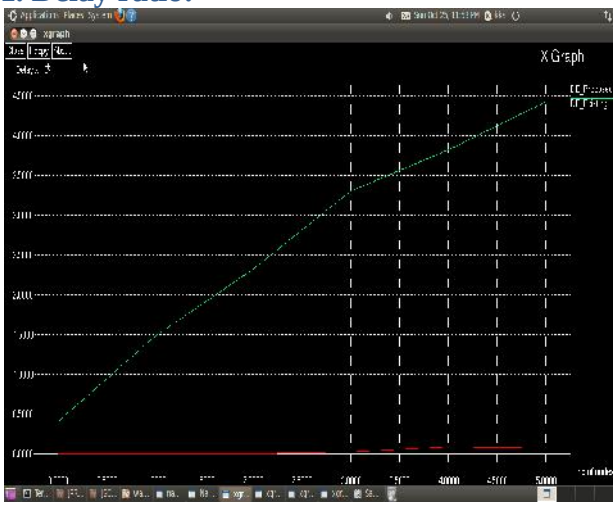
6.3. SIGNING OF SIGNATURE & VERIFICATION

The key generation procedure is used to generate the keys that are used by the signing procedure and the verifying procedure. Each time it is used the procedure generates a key pair consisting of a Private/signature key and the corresponding Public/verification key. It is important to note that the key generation procedure uses a random number generator and will generate a different pair each time it is used. SK is always known as the secret key because in applications the signing key is kept secret. PK is always known as the public key, the verification key is distributed to all users who want to verify signatures. The producer generates a signing process to transform/change the data from its original format to a new protected form. Each time it is used the procedure takes as input a signature key generated using the key generation procedure and data from some pre-determined data space. The signing procedure transforms the data and produces a signature as an output for the producer or the legal owner.

7. EXPERIMENTAL ANALYSIS AND RESULTS-D2C2

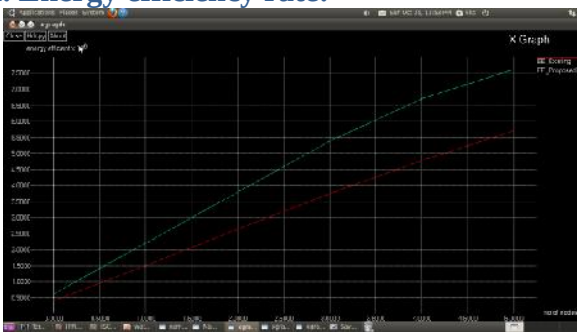
The performance of our proposed process of Delay ratio, jitter ratio, Bandwidth ratio, energy efficiency rate are comparing to existing and proposed work.

1. Delay ratio:

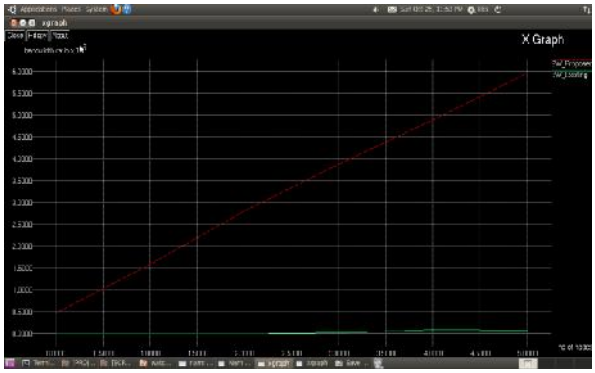


Above figure mention delay ratio of our proposed and existing comparison.

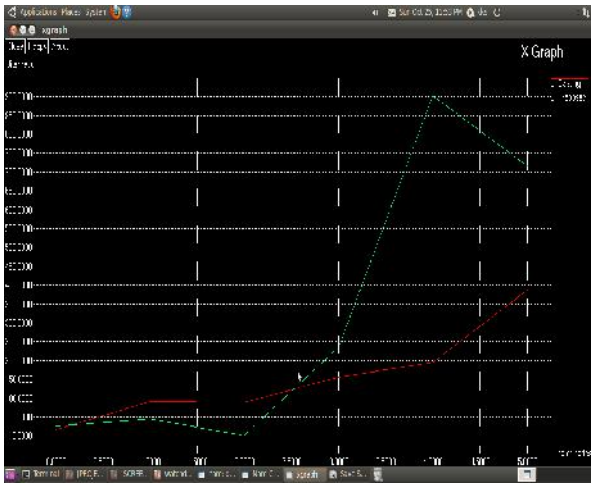
2. Energy efficiency rate:



3. Bandwidth ratio



4. Jitter ratio:



7.1. RESULTS

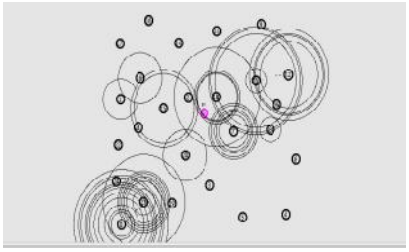


Figure 7.1- Node Initialization

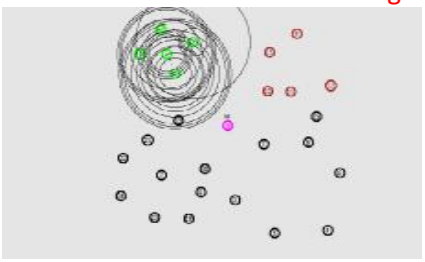


Figure 7.2- Neighbor node selection for clustering

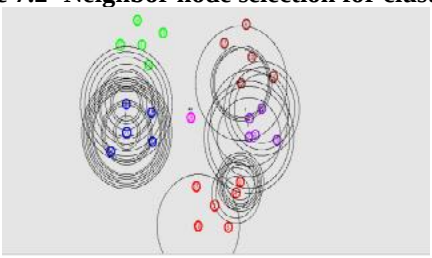


Figure 7.3- Clustering of all nodes

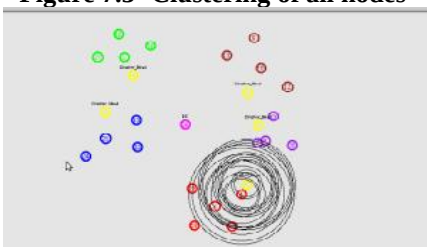


Figure 7.4- Cluster head selection process

Figure 7.5- Source and destination route selection

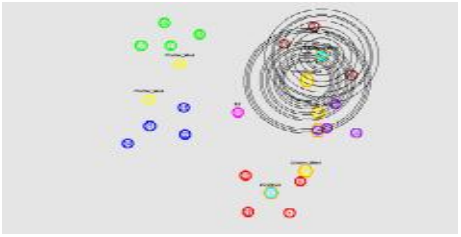


Figure 7.6- Data transmission between source and destination

Figure 7.7- Data shared without malicious

CONCLUSION

In our proposed frame work, use hybrid techniques are clustering scheme and RKP for improve network life time and security In this paper, we propose and evaluate an energy efficient clustering scheme for periodical data gathering applications in WSNs. In the cluster head election phase, based on either symmetric-key cryptosystems or public-key cryptosystems. In our proposed using RKP (Random Key Pre-distribution) .RKP schemes have several variants. Their system works by distributing a key ring to each participating node in the sensor network before deployment. We propose a key management scheme that relies on probabilistic key sharing among nodes within the sensor network. This frame work achieves high security, more energy efficiency, high packet delivery ratio, only less delay, comparing to previous frame works.In future, improve this process security as digital signature security frame work and our proposed security scheme for centralized topology networks, so in future we improve this security using digital signature security technique for decentralized large level networks topologies.

REFERENCES

[1] M. Ramkumar, N. Memon, R. Simha, "Pre-Loaded Key Based Multicast and Broadcast Authentication in Mobile Ad-Hoc Networks," Globecom- 2003.

[2] T. Leighton, S. Micali, "Secret-key Agreement without Public-Key Cryptography,"Advances in Cryptology - CRYPTO 1993, pp 456-479, 1994.

[3] R. Blom, "An Optimal Class of Symmetric Key Generation Systems," Advances in Cryptology: Proc. of Eurocrypt 84, Lecture Notes in Computer Science, 209, Springer-Verlag, Berlin, pp. 335-338, 1984.

[4] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, M. Yung, "Perfectly-Secure Key Distribution for Dynamic Conferences," Lecture Notes in Computer Science, vol 740, pp 471–486, 1993.

[5] T. Matsumoto, M.E.Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, IT-22(6), Dec. 1976, pp.644-654.

[6] P. Erdos, P. Frankl, Z. Furedi, "Families of Finite Sets in which no Set is Covered by the Union of M Others," Isreal Journal of Mathematics, 51, pp 79–89, 1985.

[7] L. Gong, D.J. Wheeler, "A Matrix Key Distribution Scheme," Journal of Cryptology, 2(2), pp 51-59, 1990.

[8] C.J. Mitchell, F.C. Piper, "Key Storage in Secure Networks," Discrete Applied Mathematics, 21 pp 215–228, 1995.

[9] M. Dyer, T. Fenner, A. Frieze and A. Thomason, "On Key Storage in Secure Networks," Journal of Cryptology, 8, 189–200, 1995.

[10] D. R. Stinson, T. van Trung, "Some New Results on Key Distribution Patterns and Broadcast Encryption," Designs, Codes and Cryptography, 14 (3) pp 261–279, 1998.

Dr. (Mrs.)N.Umadevi working as Head in the Department of Computer Science and Information Technology, Sri Jayendra Saraswathy Maha Vidyalaya College of Arts and Science, Singanallur, Coimbatore has 3 years of industrial experience and 15 years of teaching experience. Her area of interest are Image Processing and Data Mining. Her publications include 10 International Journal and 8 National Conferences.

M. MANOJ KUMAR. M. Phil Research Scholar in the Department of Computer Science, Sri Jayendra Saraswathy Maha Vidyalaya College of Arts and Science, Singanallur, Coimbatore.