Cluster Structure Based Energy Efficient Improvement for MANET

K.Prasanth, P.Sivakumar

Abstract--Mobile sinks (MSs) are very important in many wireless sensor network (WSN) applications for efficient data gathering, restricted sensor reprogramming, and for characteristic and revoking compromised sensors so, This paper presents a secure and energy-efficient geocast forwarding for MANET based on a hierarchical clustered structure with reduction of packet dropping from the base station(BS) and access point(AP), all nodes placed in one or more geocast regions. Our protocol is composed of two major parts which are protects from attackers and allow overall energy savings. First of all the hierarchical formation based on cliques and a concept of data aggregation allows us to build a robust, fast and secure foundation for routing of information, Next geocast diffusion itself is simply provide data forwarding and reduced a research phase in the network that is a step of sending data(s). Our protocol performs better in terms of less broadcast rounds overhead than the one in [38]. For security a three-tier general framework is used, that permit utilize of any pair wise key predistribution plan as its indispensable component. To decrease the compensation caused by reproduction attacks we encompass strengthened the authentication device between the sensor nodes and the stationary access node (AP) in the planned framework. Through The analysis is done using network simulator 2 (NS2) it is a packet level simulator with trace level analysis.

Index Terms-- Energy consumption, geocast forwarding, hierarchical clustering, security, MANET, three-tire, access point.

1 INTRODUCTION

The wireless sensor networks (WSN) are beginning the family of mobile ad-hoc (MANET), other than have extra features and constraints: characteristically, they consist of a wide range of sensors with limited energy capacity. Each sensor is powered from a battery non-rechargeable and non replaceable [5] and has a low capacity in terms of memory, calculation (CPU), and transmission range. For example we can mention the monitoring of forests, health monitoring [10], critical infrastructure, habitat monitoring [5], or the detection of biochemical agents and in the military industries, data acquisition in hazardous environments. Some examples of work can be found through [4, 5, 33,46]. sybil attack [11], wormhole attack [19], selective forwarding [20], [22], sinkhole [23]), and rising the energy spending at nodes close to the base station, dropping the lifetime of the system.

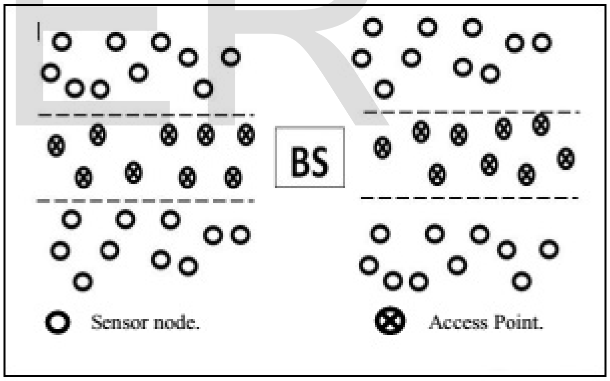

Fig. 1. Three-tire security model.

In such a system, the security is a critical position to we require revising and putting onward. In detail, WSN contain numerous constraints such as the communication standard, which is wireless: at the present time it is extremely straightforward to understand, catch and smooth adapt the information transmitted, in addition to concession an entire system. Permit us insert to these inconveniences the sensors Submission framework, which are frequently deployed in aggressive environments. Thus in attendance is a want to secure the protocols, in categorize to assurance authentication, interactions privacy [50, 39], data reliability and network accessibility. Established

----

- *Prasanth. K is currently pursuing masters degree program in embedded system technologies in SKP Engineering college, Tiruvannamalai, PH-9578505124. E-mail: kprasanthkrishna@yahoo.com*
- *Dr. P.Sivakumar is working as a professor/head dept of electronics and communication in SKP Engineering college Tiruvannamalai, E-mail: sivakumar.poruran@gmai.com.*

schemes in ad hoc networks with asymmetric keys are costly due to their computation cost and storage. These boundaries build key predistribution scheme [50] the tools of alternative to tender low cost, protected communication stuck between movable sensor sinks. So we provided the three-tier [2] security system to avoid above constrains in the network. The above figure (1) shows the simple three-tier system.

In this article we examine a process of transmitting information, the geocasting (or geographical forwarding) that guarantees the information deliverance to every sensor positioned at one or more than a few exact location of a network(geocast regions).To reach this objective we superpose to data aggregation clustered architectures. The clustered is formed based on energy in the cluster structure used as the cluster of Level 1[1] and clusters of Level 2[1] and superior. The arrangement provided by the employ of clusters allows the use of dissimilar approach compared to what is normally optional in the literature. The protocol that we present takes the main lines of [26], but is protected and intelligent to shun a preponderance of attacks [14]. Certainly, in adding together to combining the indispensable feature of security, our protocol is energy-efficient. The multi cluster arrangement in which is based our protocol helps to reduce the broadcast overhead to the local structures move toward with positive geocast regions proposed in [38] that yield huge broadcast rounds overhead.

This paper is prepared as follows. Section 2 presents geocast forwarding performed in base station, access point and within a cluster. Section 3 presents the cluster structure formation with selection of cluster head. Section 4 describes three-tire security scheme. Section 5 discussed about the stimulations. Section 6 shows about the performance measure using X-graph.

2. GEOCAST FORWARDING

The geocast forwarding is initializing in the source node to the access point then access point will examine the authentication to particular information then it passed to the base station then base station will distribute to other access point. We present two narrative algorithms for geocasting in wireless networks. The initial algorithm Geographic-Forwarding-Geocast (GFG)[40] has roughly finest Minimum overhead and is idyllic for opaque networks. The second algorithm Geographic Forwarding-Perimeter-Geocast (GFPG)[34] provides assured delivery in associated networks level at low concentration or asymmetrical distributions through gaps or obstacles.

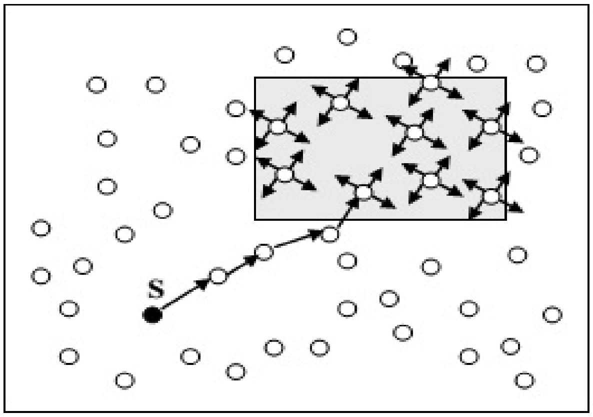

Fig. 2. Geocast forwarding in region.

2.1. GEORAPHIC FORWARDING GEOCAST(GFG)

A node wishing to throw a geocast creates a packet and puts the coordinates of the section in the frame header. Then it forwards the packet to the neighbor adjoining to the target. The target of geographic routing in this container is the section center. Apiece node sequentially forwards the information to the neighbor closest to the target using greedy forwarding Figure (2). When greedy forwarding fails, perimeter routing is worn to direction roughly dull trimmings until quicker nodes to the target are found. Eventually (in holder present are nodes surrounded by the region) the information will enter the region. The primary node to accept the geocast packet within the area starts flooding the region by broadcasting to all neighbors (otherwise we can use elegant flooding [40]). All nodes within the

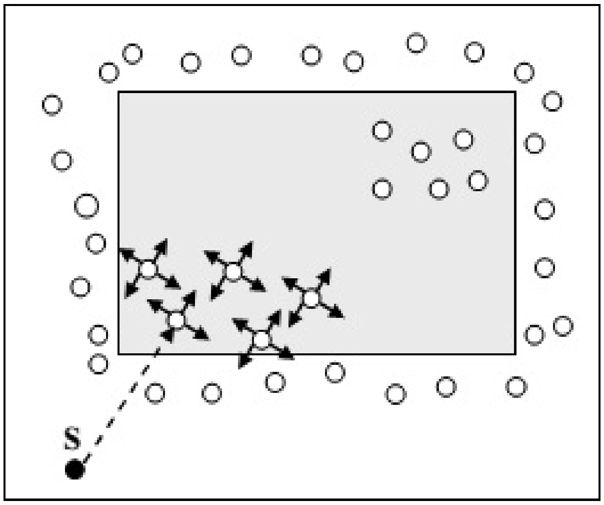

Fig. 3. Gap in Geocast region.

area that receives the information for the first time broadcasts it to its neighbors and nodes outer surface the section remove the packet. In dense networks normally this requirement is satisfied, but in sparse networks or due to obstacles, regions may have gaps such that a path between two nodes inside the region may have to go through other nodes outside the region as shown in Figure 3. In case of region gaps, GFG will fail to provide perfect delivery.

2.2.GEOGRAPHIC FORWARDING PERIMETER GEOCAST

Similar to GFG, nodes outer surface of the geocast region use geographic forwarding to forward the packet toward the area. As the packet enters the area, nodes flood it within the area. All nodes in the region broadcast the packet to their nearby nodes similar to GFG, in accumulation, nodes on the edge of the area sends perimeter mode packets to their neighbors that are outer surface of the area. A node in an area border node if it has neighbors outside of the region By sending perimeter packets to neighbors
Outside the region Figure (5).Observe that perimeter mode packets re sent only to nearby in the planar graph not to all physical neighbors. This way if the region consists of separated clusters of nodes, a geocast packet will start at one cluster, perimeter routes will connect these clusters together through nodes outside the region, and each cluster will be flooded as the geocast packet enters it for the first time.

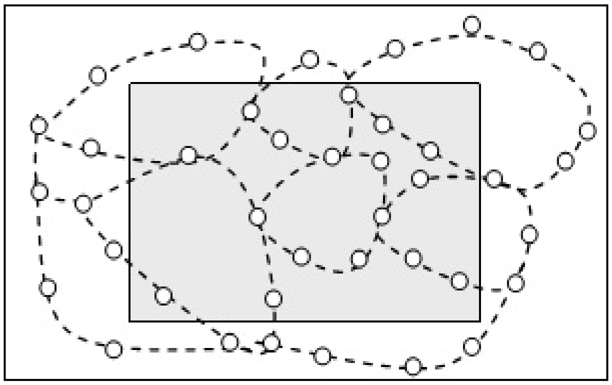

Fig. 4. Nodes connected using perimeter.

3.CLUSTER STRUCTURE

Investigate on WSNs has developed quickly and fresh techniques have been improved for the data-gathering and finding nearest path. Multihopping scheme is chosen between these techniques, which the data is routed in a cluster level manner. All nodes with the sensor in WSNs are separated into various clusters in which CHs (cluster heads) receive, information, and forward the traffic originated by cluster members to the destination. This sort of hierarchy clustering topology is simply managed and has fine scalability. Aspire is to extend the network's duration by minimizing the transmission control. However, numerous clustering protocols primarily center on stationary sensor nodes or prohibited movable for hop-count reduction in data gathering. Mobile sensor nodes are required in applications where sensors are deployed on erratically moving stuff for monitoring, tracking, and other purposes [3]. For example, wireless sensor strategies have been fixed to bikes, vehicles, and animals. Additional applications connecting humans as participants can be flu-virus tracking or air-quality monitoring. There are two algorithms to election of cluster head, Cluster-head election by counting and Cluster-head election with location.

3.1. CLUSTER HEAD ELECTION BY COUNTING

This part describes the algorithm of cluster-head election by counting. Suppose that the amount of sensor nodes in a dynamic sensor network is M and we give the sensor nodes from the count of 0 to M−1. Every sensor node therefore can use the assigned number as a single identifier (ID) in the sensor network. We suppose that there is a C cluster in each movement With the ID's, algorithm elect the sensor nodes as the cluster-heads in a round-robin method. In additional words, in the first change, the sensor nodes through ID's from 0 to C−1 are the cluster-heads. In the second change, the sensor nodes with ID's from C to 2C−1 are the cluster-heads. The algorithm continues for the next changes. After M/C changes, all sensor node has be the cluster head one time, and the total progression starts over beginning the sensor node with ID=0. The ID contains the variables t.

3.2. CLUSTER HEAD ELECTION WITH LOCATION

We here described a distributed algorithm of cluster-head election with location, which is particularly for dynamic sensor nodes. The necessary plan is to use the node mobility to have all sensor node be a cluster-head in turns. Known some fixed reference points in the location of the mobile sensor network, the sensor nodes nearby to these reference points will be the cluster-heads, correspondingly, when electing the cluster-heads. To reach this, we regard as to set the remoteness of a sensor node to a reference point (rp) as the metric of the delay time, which is worn when a sensor node contends a channel. The decision is hence also a product of the channel contention among sensor nodes. The figure given below is show the simple cluster location with group op movable sensor nodes with cluster head (CH), reference point (rp) and distance (d). Figure (5) show the cluster head election based on reference point.

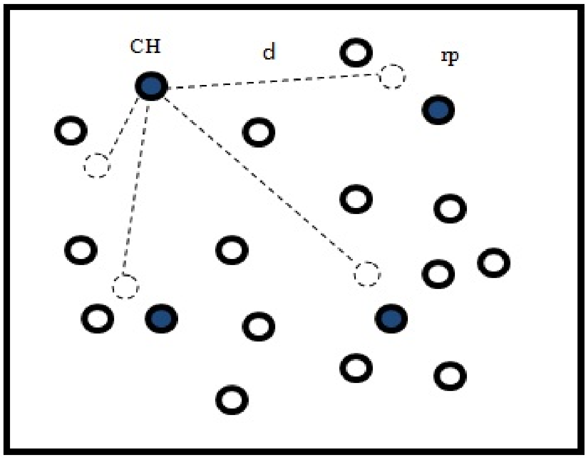

Fig. 5. Cluster head slection in location.

4. Security Scheme

For security scheme the three tire security scheme is applied. Which contains of base station, access point (AP) and finally group of dynamic sensor nodes (MANET), Dynamic sensor nodes form the cluster structure. The connection is established by AP and cluster head, which provide the authentication between these nodes. The subset of polynomials from the polynomial pool is picked by each cluster head. The randomly selected sensor nodes called access point carry a polynomial from the polynomial pool. These nodes acts as the authentication point for the network which triggers the sensor node to transmit the data. The data request is transmitted to cluster head from the sensor node through stationary access point. This data request will initiate the sensor node to transmit the collected data. Every stationary access point may share a polynomial with a mobile sensor destination. The main benefit to use pools is the mobile sensor authentication is autonomous of the key distribution scheme used to unite the sensor network. We divide our scheme into two stages: polynomial predistribution and key discovery between mobile sensor nodes.

4.1. Polynomial Predistribution

Stage 1 is performed earlier than the nodes are deployed. A polynomial pool P of size mod-P is generated along with the polynomial identifiers. All cluster head and stationary access point randomly given K_P and one polynomial (K_P>1) from P. The amount of polynomials in every cluster head is extra than the quantity of polynomials in every stationary access point. This assures that a cluster head shares a widespread polynomial with a stationary access point with high probability and reduces the number of compromised cluster head polynomials when the stationary access point shares captured. All sensor nodes and the preselected stationary access point randomly pick a subset of K_s and Ks1 polynomials from P. Blundo's Scheme[6] is the main scheme used for finding the polynomial share of each node.

4.2. Key Discovery

To set up a direct pair wise key [2] beginning one cluster head (CH1) to an extra cluster head (CH2). A cluster head (CH) want to discover a stationary access point (AP) within its range, such that AP can launch pair wise key with sensor nodes (CH). Figure (6) shows a direct secure path establishment among sensor nodes sends the pair wise key; AP between CH1 and AP. If AP receives the over message and it shares a pair wise key with CH1 it sends the pair wise key to CH2 in a message encrypted and authenticated with pair wise key; CH2 between AP and CH2.

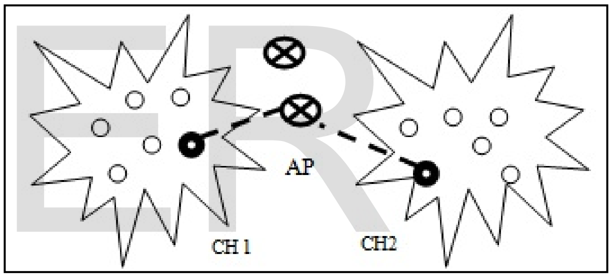

Fig. 6. Direct secure path establishment.

Figure (7) illustrate that the CH1 and the CH2 will have to establish a pair wise key with help of intermediate [2] AP using indirect key discovery. To establish pair wise key with cluster head CH2 has to find a stationary access point AP in its neighborhoods

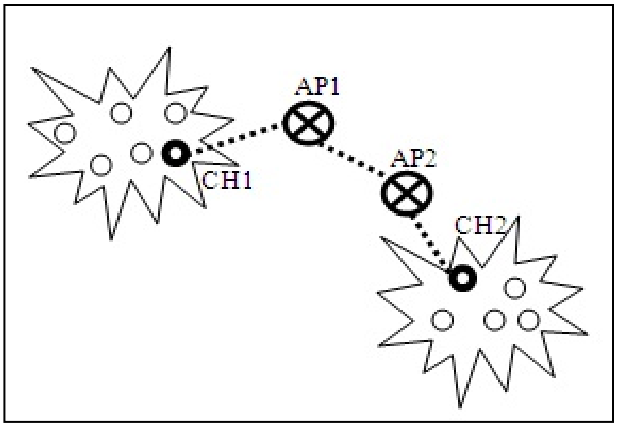

Fig. 7. Key establishment using intermediate point.

such that AP1 can establish a pair wise key with both Nodes CH2 and CH1. If AP1 establishes a pair wise key with only CH1 and not with CH2. As the probability is high that the AP1 can discover a common polynomial with CH1, CH2 need to find an intermediate AP2 along the path CH2-AP2-AP1-CH1, such that intermediate AP2 can establish a direct pair wise key with AP1.

Figure (8) Show that the cluster head and member of the cluster sensor node (n) will have to establish a pair wise key with the help of CH using indirect key discovery[2]. To establish a pair wise key with sensor node within a range of cluster head (CH2), a cluster head (CH1) has to find a stationary AP in its neighborhoods such that AP can establish a pair wise key with both CH1 and CH2. If AP establishes a pair wise key with only CH1 and not with CH2. As the probability is high that the AP can discover a common polynomial with CH1, sensor need to find an intermediate CH2 along the path n-CH2-AP-CH1,such that intermediate CH2 can establish a direct pair wise key with AP.

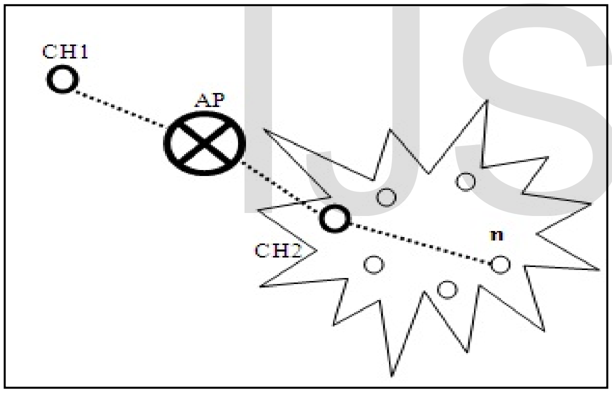

Fig. 8. Key establishment in cluster.

5. PERFORMANCE MEASURE

Performance measure is done in NS2 using awk file. AWK is an interpreted programming language designed for text processing and typically used as a data extraction and reporting tool. Awk in NS-2 takes the trace file for analysis. Handles complex task such as Calculation, database Handling, Report Creation. Awk programming can be used to analyze the metrics of any network connection. They are throughput and energy.

5.1. X-GRAPH

The graph is drawn for analyzing of performance. The graph is generated with the help of NS2 package. The graph is drawn between three tire and two tire static and dynamic security system.

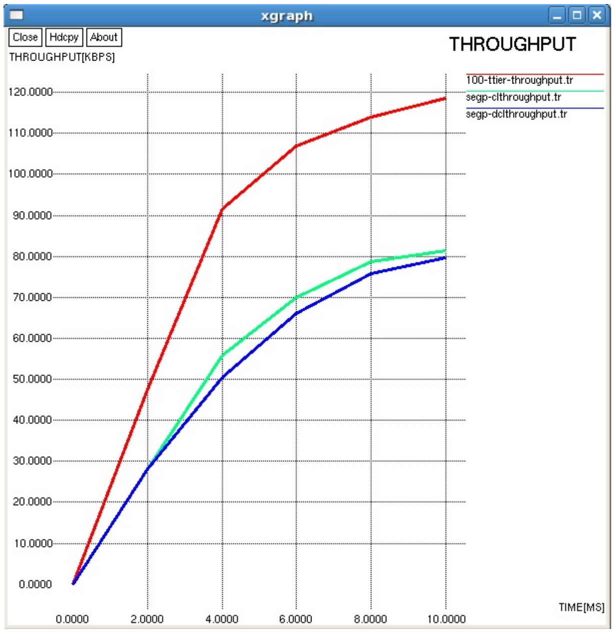

Fig. 10. Energy comparison of three-tier system with static and dynamic two-tier system.

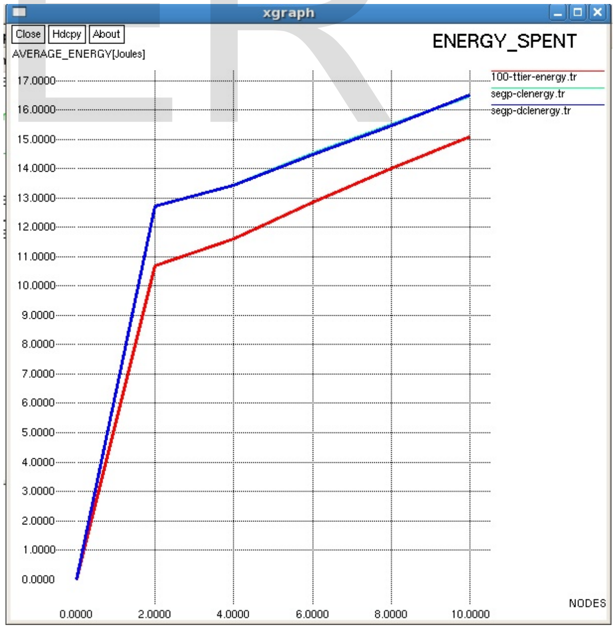

Fig. 9. Throughput comparison of three-tier system with static and dynamic two-tier system.

CONCULSION

In this document, the security scheme move towards making it promising to carry out in trouble-free and hasty manner in geocast forwarding in Base station, Access point, and in final single sensor node. The hierarchical cluster structure on which our protocol is based allows a distributed use of the network, and especially efficient use, for a control always ensured by BS, AP and cluster head. We provide distributed clustering algorithms which lead less energy dissipation for data-gathering in a cluster-based mobile sensor network. Based on the polynomial pool-based key predistribution scheme substantially improves network throughput to protracted from attacks compared to the two tire security scheme. Using separate key pools and having few stationary access point carrying polynomials from the cluster head in the network may hinder an attacker from gathering sensor data, by deploying a replicated mobile sink.

REFERENCES:

[1] S.Faye and J.F.Myoupo, "Secure and Energy-efficient Geoc-ast Protocols for Wireless Sensor Networks Based on a Hierarchical Cluster Structure," *International Journal of Network Security*, vol.15, No.3, PP.151-160, May 2013.

[2] A.Rasheed and R.N.Mahapatra, "The Three-Tire Security Scheme in Wireless Sensor networks with Mobile Sink," *IEEE Parallel and Distributed System*, vol. 23, No. 5, May 2012.

[3] Changlin Ma, Nian Liu, and Yuan Ruan, "A Dynamic and Energy-Efficient Clustering Algorithm in Large-Scale Mobile Sensor Networks" *Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks*, Volume 2013.

[4] J.Agre and L.Clare, "An integrated architecture for cooperative sensing networks," *IEEE Computer*, vol. 33, no. 5, pp. 106-108, 2000.

[5] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey," *Computer Networks*, vol. 38, no. 4, pp. 393-422, 2002.

[6] C. Blundo, A. De Santis, A. Herzberg, S. Kutt-en, U. Vaccaro, and M. Yung, "Perfectly-Secure Key Distribution for Dynamic Conferences," Proc. 12th Ann. Int'l *Cryptology Conf. Advances in Cryptology* (CRYPTO '92),pp. 471-486, 1993.

[7] S. Banerjee and S. Khuller, "A clustering scheme for hierarchical control in multihop wireless networks," in *Proceedings of the 20th IEEE IINFOCOM*, vol. 2, pp. 1028-1037, 2001.

[8] R. Blom, "An optimal class of symmetric key generation," *Advances in Cryptography- Eurocrypt' 84, LNCS 209, pp. 335-338, Springer-Verlag*, Berlin, 1984.

[9] J.S.Liu and C.H.R.Lin,"Energy-efficient clustering proto-col in wireless sensor networks," *Ad Hoc Networks*, vol. 3, no. 3, pp. 371-388, May 2005.

[10] T. Gao, D. Greenspan, M. Welesh, R.R. Juang, and A. Alm, "VitalSigns Monitoring and Patient Tracking over a Wireless Network, " *Proc. IEEE27th Ann. Int'l Conf. Eng. Medicine and Biology Soc.(EMBS)*,Sept. 2005.

[11] J.R. Douceur, "The Sybil Attack," *Proc. First Int'l Workshop Peer-to Peer Systems (IPTPS '02)*, Mar. 2002.

[12] Y. Tirta, Z. Li, Y. Lu, and S. Bagchi, "Efficient Collection of Sensor Data in Remote Fields Using Mobile Collectors," *Proc.13th Int'l Conf. Computer Comm. and Networks (ICCCN '04)*,Oct.2004.

[13] A. Rasheed and R. Mahapatra, "An Energy-Efficient Hybrid Data Collection Scheme in Wireless Sensor Networks," *Proc. Third Int'l Conf. Intelligent Sensors, Sensor Networks and Information Processing*,2007.

[14] E. Schoch, F. Kargl, T. Leinmuller, and M. Weber, "Vulnerabilities of Geocast Message Distribution," *2nd IEEE Workshop on Automotive Networking and Applications (Auto Net 2007)*, pp. 1-8, Washington, DC, USA, 2007.

[15] K.Sun, P.Peng, P.Ning and C. Wang, "Secure distributed cluster formation in wireless sensor networks," *22nd Annual Computer Security Applications Conference*, pp. 131-140. 2006.

[16] D. Niculescu and B. Nath, "Ad hoc positioning system (APS)," *in Proceedings of IEEE Global Telecommunications Conference*, pp. 2926-2931, San Antonio, 2001.

[17] V. Palanisamy and P. Annadurai, "Secure geocast in ad hoc network using multicasting key distribution scheme (SGAMKDS)," *International Association of Computer Science and Information Technology -Spring Conference*, pp. 190-194, 2009.

[18] B. Parno, A.Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," IEEE Symposium on Security and Privacy, pp. 49-63, 2005.

[19] L.Hu and D. Evans, "Using Directional Ante-nna to Prevent Wormhole Attacks," *Proc. Network and Distributed System SecuritySymp.*,2004.

[20] B.J. Culpepper and H.C. Tseng, "Sinkhole Intrusion Indicators in DSR MANETs," *Proc. First Int'l Conf. Broadband Networks (Broad Nets '04)*,pp. 681-688, Oct. 2004.

[21] Z.Ke, R.Cheng and D.Deng, NS2 Simulation Experiment, *Electronic Industry Press*, Beijing, China, 2008.

[22] H. Deng, W. Li and D.P. Agrawal, "Routing Security in WirelessAd Hoc Networks," *Proc. IEEE Comm. Magazine*, pp. 70-75, 2002.

[23] C. Intanagonwiwat, R. Govindan and D. Estrin, "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks, " *Proc. Mobi Com*,pp. 56-67, 2000.

[24] W. Zhang, G. Cao, and T. La Porta, "Data Dissemination with Ring-Based Index for Wireless Sensor Networks," *Proc. IEEE Int'l Conf. Network Protocols (ICNP)*, pp. 305-314, Nov. 2003.

[25] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U.Vaccaro, and M. Yung, "Perfectly secure key distribution for dynamic conferences," *in Proceedings of the 12th Annual International Cryptology Conference, LNCS 17*, pp. 471-486, 1992.

[26] A. B. Bomgni and J. F. Myoupo, "An energy-efficient clique-based geocast algorithm for dense sensor networks," *Communications and Network*, vol. 2, pp. 125-133, 2010.

[27] H. Chan, A. Perrig, and D. Song, "Random key predistibution schemes for sensor networks," *IEEE Symposium on Security and Privacy*, pp. 197-213, Okland California, USA, 2003.

[28] C. Y. Chang, C. T. Chang, and S. C. Tu, "Obstacle free geocasting protocols for single/multi- destination short message services in ad hoc networks," *Wireless Networks*, vol. 9, no. 2, pp. 143-155, 2003.

[29] T. Dimitriou and I. Krontiris, "A localized, distributed protocol for secure information exchange in sensor networks*," in Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium*, pp. 240a, 2005.

[30] S. F. Tzeng, C. C. Lee, and T. C. Lin, "a novel key management scheme for dynamic access control in a hierarchy," *International Journal of Network Security*, vol. 12, no. 3, pp. 178-180, 2011.

[31] A. Manjeshwar and D. Agrawal, "APTEEN: A hybrid protocol for efficient routing and a comprehensive information retrieval in WSN*," in Proceedings of the International Parallel and Distributed Processing Symposium*, pp. 195-202, Apr. 15-19, 2002.

[32] A. Perrig, R. Szewczyk, V. Wen, D. Cullar, and J. D. Tygar, "Spins: Security protocols for sensor networks*," in Proceedings of the 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking*, pp. 189-199, 2001.

[33] C. C. Shen, C. Srisathapornphat, and C. Jaikaeo,"Sensor information networking architecture and applications," *IEEE Personal Communications*, pp. 52-59, 2000.

[34] I. Stojmenovic, "Geocasting with guaranteed delivery in sensor networks*," IEEE Wireless Communications* vol. 11, no. 6, pp. 29-37, Dec. 2004.

[35] A. Wadaa, S. Olariu, L. Wilson, M. Eltoweissy, and K. Jones, "Training a wireless sensor network*," Mobile Networks and Applications*, vol.10, pp.151-168, 2005.

[36] B. Warneke, M. Last, B. Leibowitz, and K. Pister, "Smart Dust: communicating with a cubic-millimeter computer*," IEEE Computers*, vol. 34, pp. 44-51, 2001.

[37] D. Wei, S. Kaplan, and H. A. Chan, "Energy efficient clustering algorithms for wireless, sensor networks," *in Proceedings of IEEE Conference on Communications*, pp. 236-240, Beijing, 2008.

[38] Y. C. Shim, "Secure and energy efficient geocast protocol for sensor networks with misbehaving nodes," *International Journal of Communications*, vol. 2, pp. 222-229, 2009.

[39] I. A. Saroit, S. F. El-Zoghdy, and M. Matar, "A scalable and distributed security protocol for multicast communications*," International Journal of Network Security*, vol. 12, no. 2, pp. 61-74, 2011.

[40] K. Seada and A. Helmy, "Efficient geocasting with per-fect delivery in wireless networks," *IEEE Wireless Communications and Networking Conference*, pp. 2551-2556, 2004.

[41] A. Manjeshwar and D. Agrawal, "TEEN: A protocolfor enhanced efficiency in WSN*," in Proceedings of the 15th International Parallel & Distributed Processing Symposium*, pp. 2009-2015, Apr. 23-27, 2001.

[42] D. J. Malan, M.Welsh, and M. D. Smith, "A public key infrastructure for key distribution in tiny os based on elliptic curve cryptography," *SECON*, pp. 71-80, Oct.2004.

[43] J. N. AI-Karaki, R. UI-Mustafa, and A. E. Kamal, "Data aggregation in wireless sensor networks exact and approximate algorithms," *Workshop on High Performance Switching and Routing*, pp. 241- 245, Apr.19-21, 2004.

[44] Y. Hu, A. Perrig, and D. Johnson, "Packet leashes: A defense against wormhole attacks in wireless ad hoc networks," *in INFOCOM*, pp. 1976-1986, April 2003.

[45] T. Imielinski and J. Navas," GPS-Based Addressing and Routing," *RFC 2009 Computer Science, Rutgers University Press, Rutgers*, Mar. 1996.

[46] [46] C. Intanagonwiwat, R. Govindan and D. Estrin, "Dire-cted diffusion: A scalable and robust communication paradigm for sensor networks," *in Proceedings of MOBICOM' 00*, pp. 56-67, 2000.

[47] J. M Kahn, R. H Katz and K. S. J. Pister, "Mobile networking for smart dust*," in proceedings of MOBICOM' 99*, pp. 17-19, 1999.

[48] C. Karlof, N. Sastry, and D. Wagner, "Tiny Sec: A link layer security architecture for wireless sensor networks*," in Proceedings of the 2nd international conference on Embedded networked sensor systems*, vol. V, pp. 162-175, 2004.

[49] Y. B. Ko and N. H. Vaidya, "Flooding-based geocasting protocols for mobile ad hoc networks," *MANET*, vol. 7, no. 6, pp. 471-480, 2002.

[50] E. Kranakis, H. Sing and J. Urrutia, "Compass routing on geometric networks," *Proceedings of 11th Canadian Conference on Computational Geometry*, pp. 51-54, Vancouver, Aug. 1999.