IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-6, June 2018 E-ISSN: 2347-2693

A Grid Based Dynamic Symmetric Keying Protocol Based on Routing in Wireless Sensor Network

U. Durai

Department of Computer Science, Tamilavel umamaheswaranar Karanthai Arts college, Thanjavur, Tamilnadu.

**Corresponding Author: duraiu74@gmail.com*

Available online at: www.ijcseonline.org

Accepted: 14/Jun/2018, Published: 30/Jun/2018

***Abstract*—** The wireless sensor network innovation is one of the biggest information preparing and correspondence systems frameworks which consistently produced for dispersed condition in field of ongoing application. There are such huge numbers of factor related with it's as Data safety, working rate, cost proficiency and extra sensor organize imperatives. Principle thought is about increment the security over existing attacks without influence the execution and many-sided quality of general remote sensor organize. In this research, at first a protected correspondence key trading procedure for WSN called Grid Based Dynamic (GBSD) symmetric keying Protocol. Where in GBSD every sensor in a sensor organize shared symmetric keys to discuss safely with each other. In GBSD, demonstrates the Dynamic keying approach for sensor arranges that necessities to store shared symmetric keys to every sensor. This is near the ideal number of shared symmetric keys for any key dispersion conspire that isn't defenseless against agreement. In this research achieves low energy consumption, secure way of data transmission, less traffic rate in data transmission.

***Keywords*—** Public Key Cryptography, Grid Based Dynamic symmetric keying protocol, Wireless Sensor Network.

I. INTRODUCTION

The wireless sensor networks are one of the biggest developing innovations in territory of information preparing and correspondence organizes today. It is a dispersed savvy organize framework which can accord nature to finish allotted errands freely and productively because of the tremendous capability of sensor systems to empower applications that associate the physical world to the virtual world. Every node comprises of handling ability utilizing at least one microcontrollers, may contain different sorts of memory, have a RF handset, have a power source, and suit different sensors and actuators. There are numerous security plans have been recommended for WSN, yet the decision of security display in light of various properties, assurance level, and casing positions.

The key assessment measurements for WSN are lifetime, scope, cost and simplicity of arrangement, reaction time, transient exactness, security, and powerful example rate [1].
The significant themes in remote sensor arrange security, and present the deterrents and the prerequisites in the sensor security, order a considerable lot of the present assaults, and their relating guarded measures. Be that as it may, the convention ought to be flexible against false information infused into the system by pernicious nodes and bootstrap secure correspondence through utilization of key foundation instruments. Distinctive security strategies are presented for outlining taken a toll proficient, vitality productive convention for remote sensor organize like. Secure steering, cryptography, get to control convention and dynamic vitality based encoding. One of most essential research issue in WSN is the means by which to anchor the sensor arrange topology and its correspondence system from potential changes that can be made by pernicious nodes inside the current system. These remote sensor arrange are comprising little sensor that truly endure the absence of preparing capacity, memory necessity and battery control use.

There are numerous assaults presenting on this framework like attack, Sybil attack, selective forwarding, impersonation attack and convention particular attack on the information bundle of correspondence organize [3]. In this way, plan of sensor system ought to be proficient with various attributes to manage physical compels of design. There are a few strategies that are utilized by numerous analysts, subsequent to assessing a few papers it is discovered that assortment of strategy related with sensor system to anchor information transmission like. Cryptographic calculation, Network layer convention, Physical MAC control and steering procedure. Along these lines, ongoing advances in innovation have prepared for the outline and usage of new ages of the security calculations.

The security of wireless sensor networks is a challenging and exciting issue that has attracted a great deal of attention and resulted in many solutions. These solutions considered both symmetric and asymmetric key-based algorithms [2]. For instance, recent works questioned the long-standing assertion

that public key cryptography (PKC) is inefficient on resource-constrained sensor nodes; on the contrary they have demonstrated the relevant efficiency. These results establish that the potential remains for typical PKC issues to be studied along with other issues motivated by the characteristics of WSNs, including the design of new public key primitives that are suitable for resource-constrained WSNs, in addition to conventional public key problems such as key authentication, key revocation, and key distribution.

II. RELATED WORK

Security in Wireless Sensor Networks: Issues and Challenges

In this research, wireless sensor network (WSN) is a developing innovation that shows extraordinary guarantee for different advanced applications both for mass open and military. The detecting innovation joined with handling force and remote correspondence makes it lucrative for being abused in plenitude in future. The encryption-unscrambling methods conceived for the conventional wired systems are not doable to be connected straightforwardly for the remote systems and specifically for remote sensor systems. WSNs comprise of minor sensors which truly experience the ill effects of the absence of preparing, memory and battery control. Applying any encryption plot requires transmission of additional bits, henceforth additional preparing, memory and battery control which are vital assets for the sensors' life span. Applying the security systems, for example, encryption could likewise expand deferral, jitter and bundle misfortune in remote sensor systems. A large portion of the assaults against security in remote sensor systems are caused by the addition of false data by the traded off nodes inside the system. For guarding the incorporation of false reports by traded off nodes, a methods is required for recognizing false reports. In any case, growing such an identification system and making it effective speaks to an extraordinary research challenge. Once more, guaranteeing all-encompassing security in remote sensor arrange is a noteworthy research issue. Huge numbers of the present proposed security plans depend on particular system models.

Security in Wireless Sensor Networks

In this research, introduce a far reaching diagram of different security issues in WSNs. In the first master plot the imperatives of WSNs, security necessities in these systems

different conceivable assaults and the relating countermeasures. At that point an all-encompassing perspective of the security issues is introduced. These issues are ordered into six classifications: cryptography, key administration, secure directing, secure information conglomeration, interruption recognition and trust administration. The focal points and hindrances of different security conventions are examined, looked at and assessed. Some open research issues in every one of these zones are likewise talked about. Despite the fact that exploration endeavors have been made on cryptography, key administration, secure directing, secure information collection, and interruption recognition in WSNs, there are still a few difficulties to be tended to. In the first master, the choice of the suitable cryptographic techniques relies upon the handling ability of sensor nodes, showing that there is no bound together answer for all sensor systems. Rather, the security instruments are exceptionally application-particular. Second, sensors are described by the limitations on vitality, calculation capacity, memory, and correspondence data transfer capacity. The plan of security benefits in WSNs must fulfill these limitations.

Secure Routing in Wireless Sensor Network

In this research, regularly unattended and threatening arrangements of WSNs and their asset obliged sensor gadgets have prompted an expanding interest for secure vitality proficient conventions. Steering and information conglomeration get the most consideration since they are among the everyday organize schedules. With the consciousness of such request, found that so far there has been no work that spreads out a safe directing convention as the establishment for a safe information conglomeration convention. A WSN setting, a node'sid, which is freely known, is utilized to infer its open key. In non-intelligent key understanding plan, any two nodes utilize other node's id and determine a common mystery without imparting. This shared mystery, obscure to some other nodes, can be utilized to produce a cryptographic key for secure correspondence between the nodes under thought. Despite the fact that regardless it experiences the high-calculation cost of matching, it is promising in light of the fact that there has great research results for sensor organize applications.

Energy Efficient Grid based Routing Protocol

In this research, an Energy effective Grid-based directing convention with better conveyance proportion steering convention that is suited for grided sensor systems. It utilize isolating the sensor arrange field into matrices. Inside every lattice, one of the sensor nodes is chosen as a master node which is in charge of conveying the information produced by any node in that grid and for directing the information got from other master nodes in the neighbor grid. A vitality proficient Grid Based multipath directing convention with better conveyance proportion is intended to address two primary critical issues in remote sensor systems: broadening system lifetime and steering ongoing activity. Besides, to accomplish unwavering quality through giving better

conveyance proportion. Reenactment comes about have demonstrated that our proposed convention expands the existence time of the sensor system and leftover vitality is more contrasted with other convention. In the meantime it is dependable through giving better conveyance proportion.

III. EXISTING SYSTEM

In existing system, ARAN comprises of a fundamental accreditation process took after by a course instantiation process that ensures end-to-end validation. The convention is straightforward contrasted with most non-anchored impromptu steering conventions. Course revelation in ARAN is refined by a communicated course revelation message from a source node which is answered to unicast by the goal node, with the end goal that the directing messages are validated at each bounce from source to goal, and in addition on the switch way from the goal to the source.

Disadvantage

- Less security for data transmission.
- High energy consumption.
- Traffic occur in data transmission stage.

IV. PROPOSED SYSTEM

In proposed grid based dynamic symmetric keying protocol, protocol could be separated into three stages: Grids development stage, building directing table's stage, information transmission stage, time synchronization and false node detection. It first gives early on framework key data about secure information in WSN, which prompts another five meaning of key capacity. These Key capacities store the symmetric key for every sensor node without loss of simplification in the system. The keying convention requires each procedure to store not in excess of one key past the quantity of keys that should be put away in each procedure by the best uniform keying convention.

Advantage

- In proposed protocol provide a high level of security for data transmission stage.
- Less energy consumption and traffic rate.

V. METHODOLOGY

Grid Based Dynamic symmetric keying protocol

This examined Grid Dynamic symmetric keying convention depends on cryptographic key administration strategy. It first gives early on framework key data about secure information in WSN, which prompts another five meaning of key capacity. These Key capacities store the symmetric key for every sensor node without loss of simplification in the system. The keying convention requires each procedure to store not in excess of one key past the quantity of keys that should be put away in each procedure by the best uniform keying convention. This part additionally proposed a GBSD grid arrangement demonstrated as Cartesian item set and check inter master issue for an enemy to debilitate any pressure based security arrangement.

This part presumed light weight calculation the principle periods of a GBSD based keying convention. The usefulness of the proposed convention could be separated into three stages: Grids development stage, building directing table's stage and information transmission stage, time synchronization, false detection. The framework keying convention has two focal points (over the probabilistic convention). In the first master, this convention can safeguard against pantomime (not at all like the probabilistic convention) and can guard against spying (like the probabilistic convention). Second, every sensor in this convention needs to store just O(log n) symmetric keys, where n is the quantity of sensors in the system.

After forming the grids, the sink initiates a flooding message to enable the master nodes to discover the available paths from each grid to the sink. The Sink Location can be four possible cases: Sink locates at top left corner, Sink locates at top right corner, Sink locates at bottom left corner, Sink locates at bottom right corner. In our case sink is located at the top left corner of the topology. Grid density is nothing but the total number of nodes in each grid. Grid density is also calculated. The node ID filed records the node ID from which the flooding message is broadcasted. The Master node field determines the master node id for the grid specified by grid ID field. The grid has two types, boundary grids and non-boundary grids. The Hop count (H) field determines the number of hops the grid is far away from the sink. The Grid density records the total number of nodes in the grid.

The source node surges the node authentication request for (NAREQ) bundles through quick neighbours towards goal. When it achieves the goal, it sends back Authentication answer (NAREP) in the switch way. The way points of interest are put away in the grouping directing table. The clock beat field is introduced to the time.

$$O(1)=S(tn)= GDTL\ (t1)=Ti,\ ADTF\ (t1)=Tj > Tt,Tk.$$

Per hop distance field can be changed by intermediary nodes but timestamp field cannot be altered by any other nodes. The presence of malicious node can be detected by calculating the distance between each hop in a path. Consider the clock pulse time to calculate the per hop distance. CPS is defined as NAREQ and NAANS propagation time between the source and destination. Let us consider the CPS calculation between two nodes A and G where both the nodes are non-adversary nodes. The calculation time is performed during the route time discovery process in order to reduce the routing distance. Each node must run the same distance calculation using threshold value and store 60 the negligible in fact estimates O(t1+t2+t3…tn) per hop distance value in packet header.

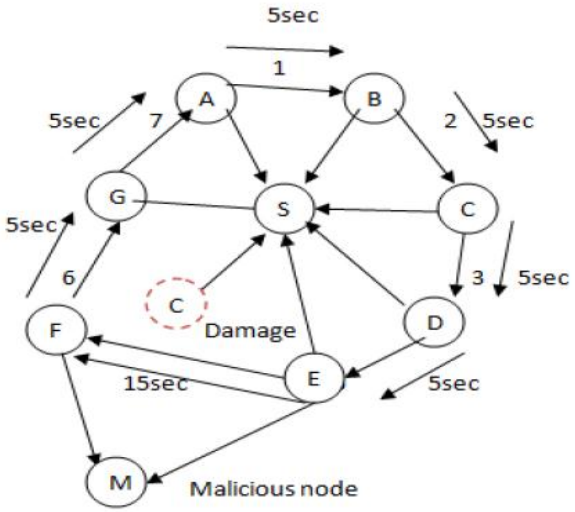

Fig 1: Detect the malicious Node

Symmetric key denoted K x, y (or) K y, x. The sensor x authenticates y and sensor y authenticates x, then Confidential Data exchange to Encrypt and Decrypt between X & Y.

Total number of sensor allocated in the network Xn.

A=f(X1, X2, X3…….Xn)

Sink node only allocate TEMP key in all sensor node

X1=2(TEMPK (2))
X2=5(TEMPK (5))…..Xn

Two condition to generate private unique key,
ix iy and (iy-ix) n/2
ix iy and (ix-iy) n/2 N=5, 0, 1,2,3,4..

The ix is between iy, iy is below ix two distinct sensor is true. Then,

SEN Keyix, iy
REN<= (A [0….n-1])
K=iy-ix < n/2 //ix below iy, if (ix<iy)

Find the malicious node

if (GDTL =T && ADTF> Ti)
CGA+CAG+Oab=O (1)
CGA+RAG=Oab=5sec+5sec=10sec
10sec=10sec
15sec(CGA+RAG) =Oag
15sec(5+5) =150(Time fault)150>10(Malicious node occur)

In the building up the routing tables, node can begin transmitting their information to the sink. In any framework, each non master node transmits its information bundles to the master node. The master node in turns chooses the appropriate next master node to forward the information to another node.

VI. RESULTS AND DISCUSION

In this results show that grid based dynamic symmetric keying protocol is unrivalled in sparing nodes vitality, expanding system lifetime, secure method for information transmission. A normal leftover vitality amid various purposes of recreation time. The vitality sparing in the proposed convention originates from the different vitality mindful plans that are utilized. To start with, not all nodes take part in ways foundation stage; only one node for each lattice communicates/gets framework based directing data. Second, non-master node sends any accessible information to the lattice master node, which handle directing. In spite of the fact that this channels master node vitality it spares grid node vitality. Third, after recognizing topology changes, (for example, when a framework ends up exhaust or when a region ended up congested) few control messages are traded between the included master nodes without flooding the system with refresh messages. It's worth to say that these topology refresh messages are traded on request not intermittently. Forward, the manner by which the ways are built up (corner to corner for non-limit and vertical/level for limit) intends to use the matrices vitality equally. This is less amount of energy consumed by MICAZ Mote devices during the periods of transmitting, receiving, idle and sleep.

Energy Consumption

In this result shows that, Secure and Energy-Efficient Multipath protocol provide a 80% of energy consumption in this research work.

An Authenticated routing for ad hoc networks provide a 50% of energy consumption in this research work. A Grid Based Dynamic symmetric keying protocol provide a 30% of energy consumption in this research work. Our proposed Grid Based

Dynamic symmetric keying protocol provide less energy consumption compared with other approach.

Table 1: Analysis the Energy Consumption

Approach	Energy Consumption
Secure and Energy-Efficient Multipath protocol	80
Authenticated routing for ad hoc networks	50
Grid Based Dynamic symmetric keying protocol	35

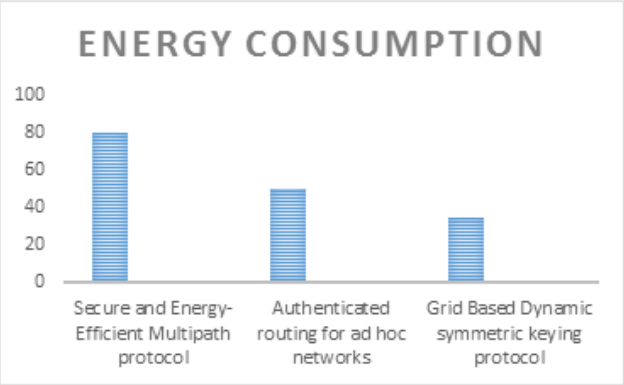

Fig 2: This Result Show that the Energy Consumption level

Traffic Rate

In this result shows that, Secure and Energy-Efficient Multipath protocol provide a 70% of traffic rate in this research work. An Authenticated routing for ad hoc networks provide a 60% of energy consumption in this research work. A Grid Based Dynamic symmetric keying protocol provide a 30% of energy consumption in this research work. Our proposed Grid Based Dynamic symmetric keying protocol provide less energy consumption compared with other approach.

Table 2: Measure the Traffic rate

Approach	Traffic Rate
Secure and Energy-Efficient Multipath protocol	70
Authenticated routing for ad hoc networks	60
Grid Based Dynamic symmetric keying protocol	30

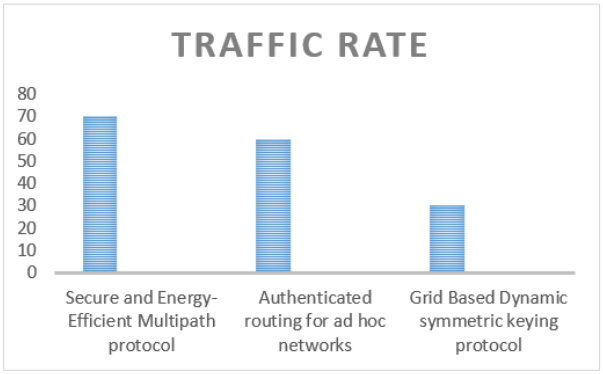

Fig 3: Relationship between varies protocol and Traffic rate

Security

In this result shows that, Secure and Energy-Efficient Multipath protocol provide a 50% of Security in this research work. An Authenticated routing for ad hoc networks provide a 60% of security in this research work. A Grid Based Dynamic symmetric keying protocol provide an 85% of security in this research work. Our proposed Grid Based Dynamic symmetric keying protocol provide high security compared with other approach.

Table 3: Analysis the Security Level

Approach	Security
Secure and Energy-Efficient Multipath protocol	70
Authenticated routing for ad hoc networks	60
Grid Based Dynamic symmetric keying protocol	30

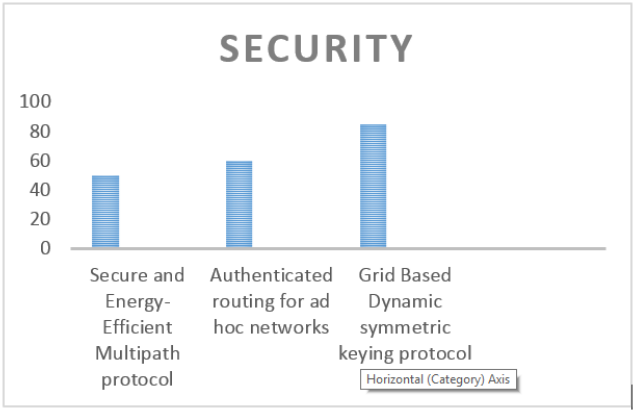

Fig 4: This experiment Show that Security Level

VII. CONCLUSION

The research work focused on planning a protected information gathering and data security considers both the exceptional steering convention that WSN has a conceivable security attack which could undermine and accumulation comes about. The proposed solution for match key also exploits the idea of key solution using a hash chain in order to achieve key secrecy. The hash chain as well as usual hash chain to provide both past and future key secrecies. The proposed GBSD security protocol provides positive features of symmetric key cryptography. GBSD creates the secrete key with reducing the malicious node and keep data freshness. In this method key generate a large odd even number after a fixed period of symmetric key to keep data integrity and avoid the replay attack.

REFERENCES

[1] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili, "*A pairwise key predistribution scheme for wireless sensor networks*," ACM Transactions on Information and System Security (TISSEC), vol. 8, no. 2, pp. 228-258, 2005.

[2] O. Yagan and A. M. Makowski, "*Modeling the pairwise key predistribution scheme in the presence of unreliable links*," IEEE Transactions on Information Theory, vol. 59, no. 3, pp. 1740-1760, 2013.

[3] F. Yavuz, J. Zhao, O. Yagan, and V. Gligor, "*On secure and reliable communications in wireless sensor networks: Towards k-connectivity under a random pairwise key predistribution scheme*," in International Symposium on Information Theory (ISIT), IEEE, 2014, pp. 2381-2385.

[4] AzrinaAbd Aziz, "*A survey on distributed Topology Control Techniques for Extending the Lifetime of Battery Powered Wireless Sensor network*", IEEE Communications Surveys & Tutorials, vol. 15, no. 1, pp. 1024-1039,2013.

[5] Benazir Fateh, "*Joint Scheduling of Tasks and Messages for Energy Minimization in Interference-aware Real-time Sensor Networks*", IEEE Transactions On Mobile Computing, pp. 1123-1136, 2013.

[6] Chatterjea,S&Havinga, P, "*A Dynamic data aggregation scheme for Wireless Sensor network," Research on Integrated Systems and Circuits"*, Veldhoven, The Netherlands, Nov. 2003.

[7] Chih-Min Chao, "*Design of structure-free and energy-balanced data aggregation in Wireless Sensor network*", ELSEVIER, Journal of Network and Computer Applications vol. 37, no. 5, pp.229– 239,2014.

[8] Chi-Tsun Cheng, "*A Delay-Aware Network Structure for Wireless Sensor network With In- Network Data Fusion*", IEEE Sensors Journal, vol. 13, no. 5, pp. 1234-1248,May 2013.

[9] Clausen, T&Jacquet, P, "*Optimized Link State Routing Protocol (OLSR)*", http://tools.ietf.org/html/rfc3626, 2003.

[10] Considine, J, Li, F,Kollios, G & Byers, J, "*Approximate aggregation techniques for sensor databases*," in Proc. IEEE Int. Conf. Data Engineering (ICDE), 2004.

[11] Cristescu, R,Beferull-Lozano,B&Vetterli, M, "*On network correlated data gathering*", IEEE Computer and Communications Societies, vol. 4, pp. 2571–2582, 2004.

[12] Dantu, K &Sukhatme, G, "*Connectivity vs. control: Using directional and positional cues to stabilize routing in robot networks*", International Conference on Robot Communication and Coordination (RoboComm'09). pp.1–6,2009.

