Journal of Engineering Sciences
Vol 11, Issue 5,May/2020
ISSN NO:0377-9254

DESIGN OF ADVANCED ROUTING PROTOCOL IN WIRELESS SENSOR NETWORKS

Dr. C. KrishnaPriya[1], Dr.P.Sumalatha[2]

[1]Assistant Professor, Department of Computer Science & Information Technology, Central University of Andhra Pradesh, Anantapuramu, 515001, Andhra Pradesh, India

[2] Assistant Professor, Department of Computer Science, Sri Vani Institute of Management and Sciences, Anantapuramu, 515001, Andhra Pradesh, India

Abstract— Basically, wireless sensor networks play a major role in industrial applications. In this paper, proposing a design of wireless sensor network to secure the information by using TSS Routing Mechanism. The wireless sensor network becoming difficult to discuss typical requirements of hardware issues and software support. For the running wireless networks selecting the nodes by using the time-oriented competition algorithm, reduces the dynamic topology of among sensor nodes instead of negotiation mechanism. The main aim is reducing the network traffic burdens. The proposed system has the ability to resist many common attacks simultaneously and at the same time the security route selection algorithm is also optimized by taking trust degree and quality of service metrics into account.

Keywords— Wireless Sensor Network, QOS Metrics, Trust Sensing Based Secure Routing Mechanism (TSSRM).

1. INTRODUCTION

Wireless sensor network can generally be delineated as an arrangement of centers that accommodatingly sense and control the earth, enabling collaboration between individuals or PCs and the incorporating condition. WSNs nowadays consolidate sensor centre points, actuator nodes, entries and clients. A tremendous number of sensor centre points sent randomly inside or near the checking area (sensor field), structure masterminds through self-affiliation. Sensor node points screen the accumulated data to transmit along to other sensor centre points by bouncing [1-3]. During the methodology of transmission, watched data may be managed by various node points to get to entry centre after multi-skip coordinating, in conclusion land at the organization node point through the web or satellite.

As related advancements build up, the cost of WSN equipment has dropped definitely, and their applications are logically stretching out from the military districts to present day and business fields. In the meantime, benchmarks for WSN advancement have been particularly developed, for instance, Zigbee, Wireless Hart, ISA 100.11a, remote frameworks for present day computerization – process robotization (WIA-PA, etc. Moreover, with new application strategies for WSN ascending in present day motorization and home applications, the full scale market size of WSN applications will continue growing rapidly.

Generally, imagining the enormous scale arrangements of wireless sensor systems for disseminated control and observing applications. These systems are made out of another class of reduced registering gadgets which coordinate minor sensors and actuators with very low-control calculation and remote correspondence. It is predicted that these gadgets will in the long run be little and reasonable enough to effectively convey on a huge scale, conceivably even blended and dispersed from airplanes.[4] Potential applications incorporate natural, restorative, and environment observing, vitality the executives, stock control, home and building mechanization, and military fighting.

It is vital that users ought not to have the option to disturb or meddle with the routing framework – without it, a sensor system is disabled and futile. Yet, the difficulties are extraordinary. Remote correspondence is innately unreliable and sensor hubs have moderate processors, constrained vitality, and almost no memory and capacity. Furthermore, numerous sensor systems will probably be sent in open, physically uncertain, or even threatening

situations.

2. RELATED WORK

Remote sensor frameworks have starting late become a power to be dealt with considering the way that they hold the likelihood to disturb various areas of our economy and life, from biological checking and safeguarding, to gathering and business asset the board, to computerization in the transportation and human administrations adventures. The arrangement, execution, and action of a sensor framework requires the point of various requests, including sign getting ready, frameworks organization and shows, embedded structures, information the board and passed on figuring's. Such frameworks are routinely sent in resource constrained circumstances, for instance with battery worked centre points running untethered. These necessities direct that sensor sort out issues are best moved closer in an undermining way, by together considering the physical, frameworks organization, and application layers and making critical arrangement tradeoffs over the layers.

Wireless sensor systems are regularly utilized in profoundly powerful, and threatening conditions with no human presence (dissimilar to ordinary information systems), and along these lines, they should be tolerant to the disappointment and loss of availability of individual hubs. The sensor hubs ought to be insightful to recuperate from disappointments with least human contribution. Systems should bolster procedure of independent development of network, tending to, and routing structures. Late inquires about on Autonomic Networking can fill in as reason for structure of Autonomic WSN. Wireless sensor systems are made out of hundreds or thousands of little measured sensor hubs that can participate in identifying physical situations. One of the benefits of remote sensor system is the capacity to work unattended in brutal condition in which contemporary human-insider savvy observing plans are unsafe, wasteful and in some cases infeasible.

Many research works have examined the issue of pernicious hub identification. The majority of these arrangements manages the discovery of a solitary malevolent hub or require gigantic asset as far as time and cost for recognizing helpful dark opening assaults. Also, a portion of these techniques require explicit situations or presumptions so as to work. At the point when all is said in done, area frameworks that have been proposed so far can be assembled into two general orders. Proactive area plans will be plans that need to constantly perceive or screen near to centers. Among the above plans are the ones proposed which consider a benchmark plans for execution examination purposes [5-8].The plan for the recognition of routing trouble making. In this plan, two-jump affirmation parcels are sent the other way of the directing way to show that the information bundles have been effectively gotten.

3. EXISTED SYSTEM

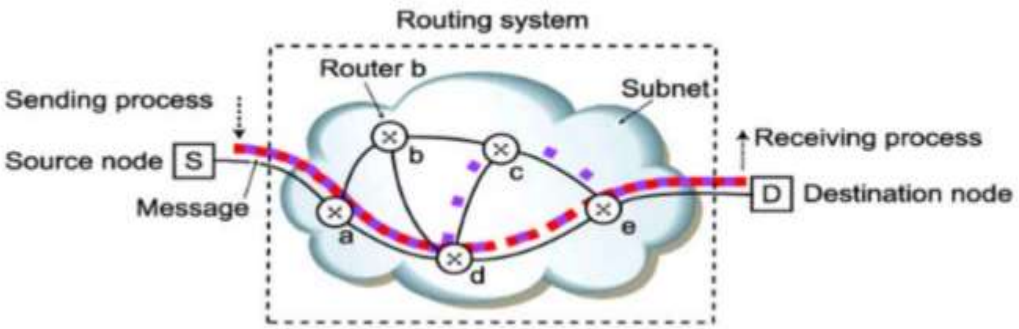

Figure 1: EXISTED ROUTING SYSTEM

The above figure (1) shows the structure of existing system. The movement and consumption of energy is observed based on the sensor nodes. The trust of the degree is

calculated based on the routing procedure. From source to destination the routing length is calculated. Keen urban areas that depend on various kinds of conveyed smart gadgets can give urban inhabitants a wide scope of utilizations, for example, ecological checking, traffic the board, and social excitement. WSN with the trait of ease, quick arrangement and self-association assumes an imperative job in encouraging the administrations of brilliant city.

The multi-jump steering is helpless against different sorts of assaults because of the open, dispersed and dynamic quality of WSN, which seriously affects information and data security. Based on trust the ordinary directing convention is hard to guarantee the security of multi jump transmission of data in the current steering convention dependent on trust has certain confinements.

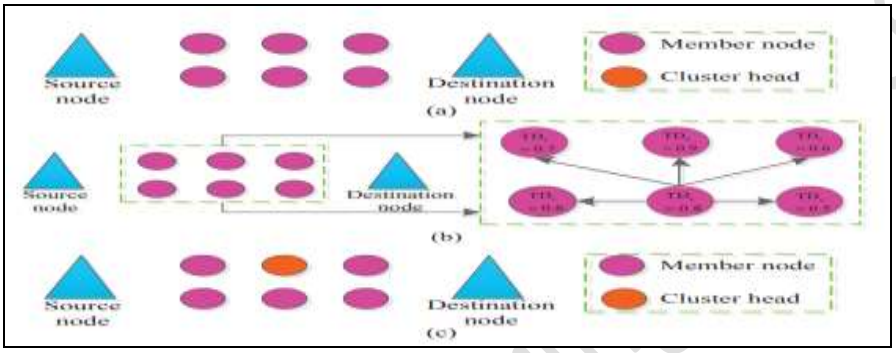

Figure 2: THE CHOICE PROCESS OF CLUSTER HEAD

The above figure (2) shows the process of cluster head. Here the hub is picked based on the group of head. From figure (2) it can observe that there are 6 hubs which are connected together based on the topology of bunching system. From figure 2(a) it can observe that degree of trust is irregular and non grouped. From figure 2(b) the degree of trust is based on the neighbour node. From figure 2(c), the correlation of hubs based on the header is shown. The upstream hub of the bombed connection starts course support to acquire another believable course to the goal hub when any connection in the course comes up short. Hub n_2 will send steering update bundles to source hub n_0 by means of turnaround course in the event that it can't locate an elective course to hub n_6 or the trust level of elective course cannot meet the imperative conditions of trust and remaking the ideal sound course.

4. PROPOSED SYSTEM

In this proposing a Trust Sensing based Secure Routing Protocol (TSSRM). This Trust Detection protocol algorithm is used to find the neighbor node of in this network. Nodal trust calculation algorithm every node will aid to avoiding the black hole during the data routing and detection routing. These modules interact closely to coordinate the functions of detecting misbehavior, discovering trusted routes, and assessing peers ' reputation. Here, considering a remote sensor system comprising of sensor hubs that are consistently and haphazardly dispersed in a roundabout system; the framework range is R, with nodal thickness ρ, and centers don't move in the wake of being passed on. Unending an event supply, message was made by a sensor centre point, and those messages must be sent to the sink node. It considers that association level security has been developed through a regular cryptography-based show.

Subsequently, this considers an association key to be protected with the exception of if the adversary physically deals either side of the association. The enemies model: it consider that dull openings are encircled by the undermined centre points and unselectively discard all packages passed by to shield data from being sent to the sink. The adversary can deal a part of the centers. Be that as it may, we believe the foe to be notable trade off the sink and its neighbouring hubs. The information accumulation has better security execution and

solid capacity against dark gap assaults.

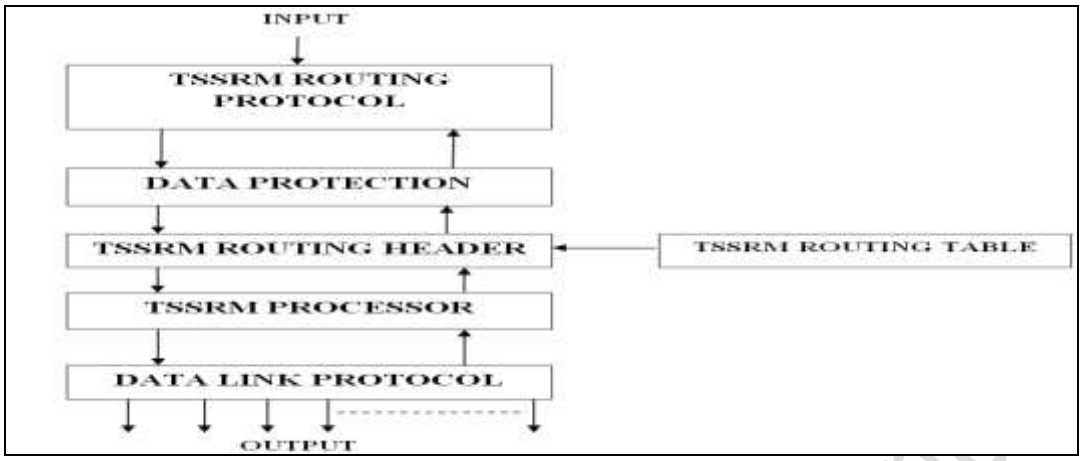

Figure 3: TSSRM BLOCK ARCHITECTURE

The figure (3) shows the block architecture of TSSRM. Here mainly TSSRM protocol, data protection, TSSRM routing header, TSSRM processor and data link protocol are used. Here first the input is given to the routing protocol to give direction and then after reaching from source to destination the data is protected. After this the data is transformed in the form of bits or bytes to header and this will be based on the TSSRM table. Now the processor will take all this data process the operation and transfer the data using data link protocol.

Here, the processed data is followed by the data link protocol. The main intent of data link protocol is to transmit the data from one node to another node. This protocol will receive the output in form of bits and bytes. Here the data is secured by ensuring the data of node from the processor. The packets number that is available in the system is represented as M and the packets which are processed by sinking process then that data is represented by m. Therefore the ratio of this measured as q=m/M. Here, the length of the route is decreased by 1 for every hop and after that the routing processor will end.

Basically, in the wireless sensor network, the routing protocol is very similar but here mainly TSSRM protocol is used. The steering convention can receive a current directing convention, and accepting the most brief course convention for instance. In the course hub will pick the neighbor, it has high trust and closer to the sink as the following bounce. On the off chance that there is no hub whole neighbor closer to the sink, trust over the default limit, this will answer to the upper hub that there is no way from to the sink. The upper hub, working in a similar way, will re-select an alternate hub from among its neighbors closer to the sink until the information are directed to the sink or there is no way to convincing the sink. The information is verified dependent on the conditions given. The centre thought of information steering is that when any hub gets an information bundle, it chooses one hub from the arrangement of competitors closer to the sink; whose trust is more noteworthy than the preset edge as the following bounce.

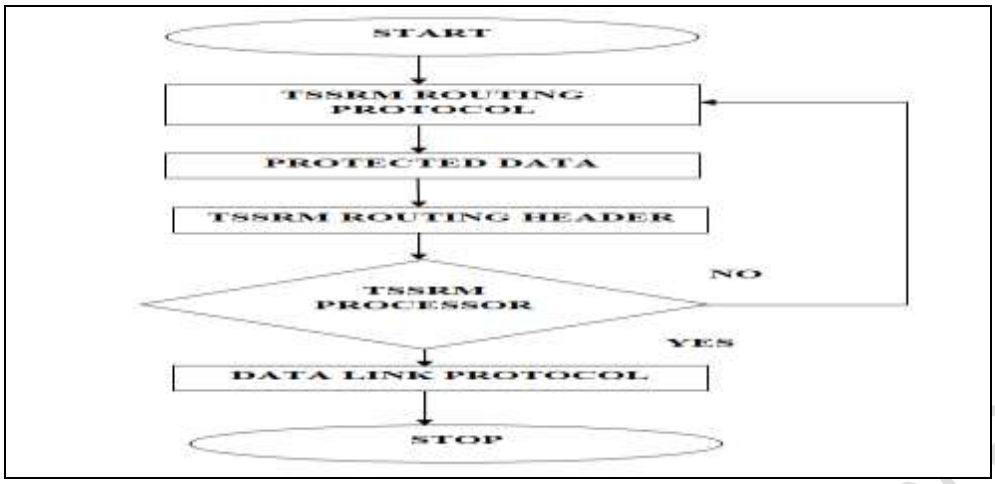

Figure 4: TSSRM FLOW CHART

The figure 4 represents the TSSRM flow chart routing protocol. This flow chart will directly derive the system to produce better communication. In there will be interaction between the nodes which are recommended. Here first input is given to TSSRM protocol. The routing protocol will process the data after applying some nodes to it. Now the data is protected using the data protection block. After protection of data, now it will passes through the routing header using TSSRM routing table. Here the TSSRM processor will accept the data only when they obtained data is related to the TSSRM. It will not accept the data when the data is not related to the TSSRM protocol and this will again send back to check the data. Hence the operation will be ended based on that condition. Hence this proposed flow chart will give routing value very less and speed of operation with high speed.

5. RESULTS

The below figure 5 shows a comparison graph of the time consumption on routing establishment.

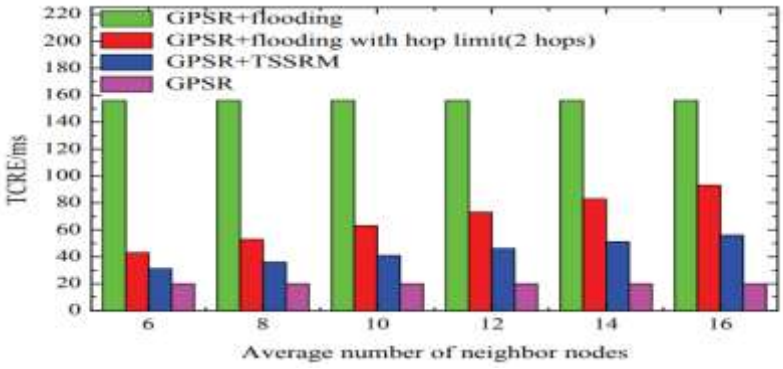

Figure 5: TIME CONSUMPTION ON ROUTING ESTABLISHMENT

The below figure (6) shows the comparison graph of routing overhead.

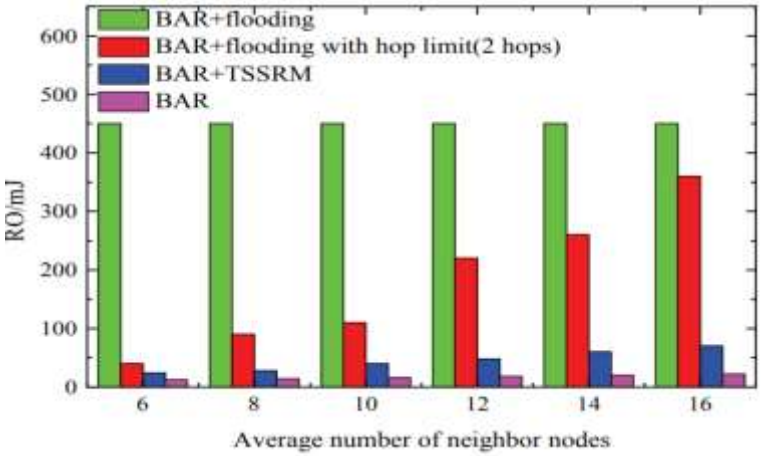

Figure 6: ROUTING OVERHEAD

6. CONCLUSION

In this paper, the development of trust based secure routing mechanism is introduced. This mechanism will overcome the attacks of common network. By using the semi ring theory concepts internally, the proposed system is optimized. This system mainly depends on the degree of trust and quality of services. The overhead routing is reduced which is observed from the simulation results. Compared to the existed routing mechanism, the proposed TSSRM will give effective reliability while transmission of data. Hence the proposed routing mechanism will give ubiquitous routing and trust degree.

REFERENCES

[1] O. Ozel, K. Tutuncuoglu, J. Yang, S. Ulukus, and A. Yener, "Transmission with Energy Harvesting Nodes in Fading Wireless Channels: Optimal Policies," IEEE Journal on Selected Areas in Communications, vol. 29, no. 8, pp. 1732-1743, September. 2011.

[2] N. Marlon, C. Jose, A. B. Campelo, O. Rafael, V. C. Juan, and J. S. Juan, "Active Low Intrusion Hybrid Monitor for Wireless Sensor Networks," Sensors, vol. 15, no. 3, pp. 23927-23952, 2015.

[3] G. Ottman, A. Bhatt, H. Hofmann, and G. Lesieutre, "Adaptive Piezoelectric Energy Harvesting Circuit for Wireless Remote Power Supply," IEEE Transactions on Power Electronics, vol. 17, no. 5, pp. 669-676, September. 2002.

[4] A. K. A. Mohammad, and S. Gadadhar, "Enhancing Cooperation in MANET using Neighborhood Compressive Sensing Model," Egyptian Informatics Journal, vol. 6, no. 1, pp. 1-15, 2016.

[5] G. Uttam G, and D. Raja, "SDRP: A Secure and Dynamic Routing Protocol for Mobile Ad-hoc Networks," IET Networks, vol. 3, no. 2, pp. 235-243, 2014.

[6] W. K. K. Chin, and K. L. AYau, "Trust and Reputation Scheme for Clustering in Cognitive Radio Networks," International Conference on Frontiers of Communications, Networks and Applications (ICFCNA), Kuala Lumpur, Malaysia, Nov. 2014, pp. 1-6.

[7] Y. Gao, H. W. Chris, J. J. Duan, and J. R. Chou, "A Novel Energy-Aware Distributed Clustering Algorithm for Heterogeneous Wireless Sensor Networks in the Mobile Environment," Sensors, vol. 15, no. 10, pp. 31108- 31124, 2015.

[8] J. G. Choi, S. Bahk, "Cell-Throughput Analysis of the Proportional Fair Scheduler in the Single-Cell Environment," IEEE Transactions on Vehicular Technology, vol. 56, no. 2, pp. 766-778, 2007.

[9] K. B. Sourav, and M. K. Pabitra, "SIR: A Secure and Intelligent Routing Protocol for

Vehicular Ad hoc Network," IET Networks, vol. 4, no. 6, pp. 185-194, 2015.

[10] E. Adel, K. Abdellatif, and E. Mohammed, "A New Trust Model to Secure Routing Protocols against DoS Attacks in MANETs," The 10th International Conference on Intelligent Systems: Theories and Applications (SITA), Taiwan, October. 2015, pp. 1-6.

AUTHORS

Dr. C. Krishna Priya, currently working as Assistant Professor in the Department of Computer Science and IT, Central University of Andhra Pradesh, Anantapuramu, Andhra Pradesh. She received her Master of Computer Applications from Sri Krishnadevaraya University, Anantapuramu, A.P., India, in 2007, M.Tech. (IT) from Karnataka State Open University, Mysore; Karnataka in 2011. She did her Ph.D. in Computer Networks in the Department of Computer Science and Technology from Sri Krishnadevaraya University, Anantapuramu, A.P., India, in 2017. She qualified Andhra Pradesh State Eligibility Test and National Eligibility Test for Lecturership in 2017, 2019 December respectively. She had 12 years of teaching experience. Her current research interest includes Computer Networks, Network Security and Intrusion Detection.

Dr. P. Sumalatha is working as Assistant Professor in the Department of Computer Science, Sri Vani Institute of Management and Sciences, Anantapuramu, Andhra Pradesh. She received her M.Sc. (Computer Science) from Sri Krishnadevaraya University, Anantapuramu, A.P., India, in 2007. She did her Ph.D. in Computer Networks in the Department of Computer Science and Technology from Sri Krishnadevaraya University, Anantapuramu, A.P., India, in 2017. Her current research interest includes Computer Networks and Network Security.