International Journal of Pure and Applied Mathematics
Volume 117 No. 21 2017, 107-112
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

A Novel Approach to Cost-Aware Energy Based Routing Protocol for Wireless Sensor Networks

S. Karthikeyan[1], M. Venkata Nagi Reddy[2], M. Mazeed Ahamed[3], V. G. Sivakumar[4]
[2,3]B.E, Student, [1,4]Associate Professor
[1,2,3,4] Department of ECE, Sathyabama University, Chenni, India

Abstract— **The main objective of this project is to supply the protection and increase the network life time. we tend to tend to selected our domain energy management in wireless detector networks to boost the protection system. A typical wireless detector network consists of the many tiny and low-power sensors that use radio frequencies to perform distributed sensing tasks. These nodes typically have really restricted and non-replenish prepared energy resources, that produces energy a vital vogue issue for these networks. Routing is another really troublesome vogue issue for WSNs. A properly designed routing protocol should not alone guarantee high message delivery magnitude relation and low energy consumption for message delivery, but to boot balance the complete detector network energy consumption, and thereby extend the detector network period. Throughout this project, we tend to tend to confer a secure and economical worth Aware Secure Routing protocol for WSNs to balance the energy consumption and increase network period. extra we tend to tend to boost very cheap work to avoid the fake position indicator nodes by victimization the area parameters.**

Keywords: Geo Routing, Energy efficiency, Security, Wireless sensor network

I. INTRODUCTION

Future detector networks area unit composed of associate outsized variety of densely deployed detector nodes. every node among the detector network might embrace one or further sensors, an occasional power radio, movable power provide, and presumably localization hardware, style of a GPS (Global Positioning System) unit or a travel device. A key feature of such networks is that their nodes ar unattended. Consequently, they need restricted and non-replicable energy resources. Therefore, energy potency could also be an important vogue thought for these networks. throughout this paper we've an inclination to tend to review energy economical geographic packet forwarding techniques. Distributive data to a section may well be a extremely helpful primitive in several location aware systems, and notably detector networks. The region may even be expressed, as associate example, by a an economical owing to publicize the geographic question to such region is to leverage the position information among the question and to route the question on to the region rather than flooding it all over. Previous analysis has studied the thanks to geographically route a packet to a target location in associate ad-hoc network. Detector networks suppose wireless communication, that is naturally a medium and is further in danger of security attacks than its wired counterpart as a result of lack of a physical boundary.

Among the wireless detector domain, anybody with a suitable wireless receiver can monitor and intercept the detector network communications.

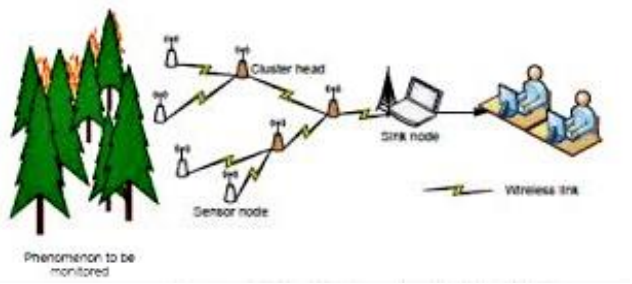


Fig 1.1: Architecture of Typical WSN

The adversaries might use valuable radio transceivers, powerful workstations, and move with the network from a distance since they're not restricted to exploitation detector network hardware. it's possible for the adversaries verify to spot} the message supply or even establish the supply location, though sturdy coding is used. Source-location privacy (SLP) could also be a vital security issue. Lack of SLP will expose important information regarding the traffic carried on the network and collectively the physical world entities. Whereas confidentiality of the message may even be ensured through content secret writing, it's plenty of adverse to adequately address the SLP. protective SLP is even more durable in WSNs since the detector nodes embrace alone low-cost and low-power radio devices, and ar designed to control unattended for long periods of it slow. Battery recharging or replacement is to boot unworkable or impossible. Computationally intensive crypto graphical algorithms, like public-key cryptosystems, and huge scale broadcasting based mostly protocols, don't seem to be acceptable for WSNs. To

optimize the detector nodes for the restricted node capabilities and collectively the appliance specific nature of the WSNs, historically, security needs were for the foremost 0.5 unnoticed. This leaves WSNs in danger of network security attacks. among the worst case, adversaries ar ready to undetectably lead of some wireless detector nodes, compromise the cryptographically keys, and reprogram the wireless detector nodes. throughout this paper, we've an inclination to tend to initial propose some criteria to quantitatively live source-location information discharge for routing-based SLP schemes. Through the projected live criteria, we've an inclination to tend to ar ready to establish security vulnerabilities of some exiting SLP schemes. we've an inclination to tend to then propose a theme matter which may offer each content confidentiality and SLP through a two-phase routing. among the initial routing section, the message provide haphazardly selects AN intermediate node among the detector domain so transmits the message to the haphazardly designated intermediate node (RSIN). This section provides SLP with a high native degree. among the second routing section, the messages square measure routed to a hoop node wherever the messages square measure homogenized through a network admixture ring (NMR). By integration the nuclear resonance, we've got a bent to ar able to dramatically decrease the native degree and increase the SLP. Our simulation results demonstrate that the projected theme is improbably economical and will come through a high message delivery relation. we've got a bent to tend to believe it's attending to be utilized in several sensible applications.

II. RELATED WORK

The main ideas of [1] authors approach were to ignore the unidirectional link at the network layer and magnificence novel shake and channel reservation mechanisms at the medium-access management layer u sing topological information collected at intervals the network layer. This paper entirely to find the unidirectional links and to avoid the transmissions supported uneven links whereas not considering the benefits from dynamic nodes. In [2] paper, author planned a cross layer framework that effectively improves the performance of the mac layer in power heterogeneous impromptu networks. to boot, our approach seamlessly supports the identification and usage of unidirectional links at the routing layer. In [3] paper author thought of the periodic greeting sharing is to hunt out the unidirectional link. but this periodic sharing might even be causes to overhead at intervals the network. In [4] paper, author planned a distributed answer supported reducing the density of the network exploitation a pair of mechanisms: bunch and adjustable transmission vary. By exploitation adjustable transmission vary; author to boot achieved another objective, energy economical vogue, as a by-product. In [5] paper, author thought of bunch mechanism. due to tightly coupled technique may increase the delay in data transmission. In [5] paper, author presents ad-hoc on demand distance vector routing (AODV), a very distinctive rule for the operation of such ad-hoc networks. each mobile host operates as a specialized router, and routes unit obtained professional re natal (i.e., on-demand) with little or no reliance on periodic advertisements. AODV is associate on demand routing protocol at intervals that routes unit established on demand and destination sequence numbers unit accustomed notice the most recent route to the destination. The affiliation setup delay could be a smaller quantity. The greeting messages supporting the routes maintenance unit range-limited, in order that they do not cause superfluous overhead at intervals the network but the intermediate nodes can end in inconsistent routes if the provision sequence selection is extraordinarily previous and conjointly the intermediate nodes have a far better but not the most recent destination sequence selection, thereby having stale entries. In [6] paper, author discuss about a mathematical groundwork for computing the overhead of proactive routing protocols in mobile networks. He focus on things where the nodes unit indiscriminately road but the wireless transmissions could also be decoded reliably, once nodes unit among communication vary of each totally different. In [7] paper, author has outlined about energy efficient system for heterogeneous wireless sensor networks. In this paper he described that heterogeneous hybrid energy efficient distributed protocol (H-HEED) is the adjusted protocol of HEED protocol that communicates between node to node. It also regenerate the network to improve overall performance. The overall energy required for reception and transmission is formulated by source and sink. According to node energy, energy levels are divided in terms of its energy required for reception and transmission of data.

A. Existing system

Several geographical routing protocols ar planned in recent years for wireless detector networks. In geographical routing each node forwards messages to its neighboring nodes supported estimated worth and learning worth. The estimated worth considers every the house to the destination and additionally the remaining energy of the detector nodes. Provide location privacy is provided through broadcasting that mixes valid messages with the dummy messages not only consumes the many of detector energy but to boot can increase the network collisions and scale back the packet delivery quantitative relation.

***Disadvantage*:**

- Power outages
- Due to Environmental disasters, loss in the information
- Lost productivity
- Various DOS and black hole attacks
- Secure level is low.

III. PROPOSED SYSTEM

We discover that the energy consumption is severely disproportionate to the uniform energy preparation for the given configuration that greatly reduces the amount of your time of the sensing element networks. To resolve this

downside, we have got a bent to propose a secure and economical Cost-Aware Secure Routing protocol that is ready to handle energy balance and routing security at identical time in WSNs. In CASER protocol, every sensing element node must maintain the energy levels of its immediate adjacent neighboring grids besides to their relative locations. Throughout this project we'll focus on a try of routing ways in which for message forwarding: shortest path message forwarding, and secure message forwarding through random walking to make routing path unpredictability for provide privacy and jam hindrance.

Energy Algorithm

####forming Network########
Create a list N(all); #A set contains all the information about nodes
Initiate forming Network
Source generate RREQ
Forward to all neighbors

If (Received by destination) {
Generate RREP
} else {
Forward to Next Nodes
}

#######Checking and Validation##########
All the nodes update the energy level to their neighbors
If (Less Energy in Routing Nodes) {
Inform Source to Regenerate RREQ
} else {
Continue the Route
}

#########Balanced Model########
Source will select the route based on balanced energy level in all the paths
If (Path has low energy modes) {
Choose Different Path
else {
Choose the same path
}

A. *Route discovery*

Initially all node assortment the information regarding neighbor nodes, the network monitors having the careful data of neighbor nodes like routing table, It provides the affiliation data to route manager.

B. Energy updating

The mobile devices periodically share their residual energy into all the nodes that area unit collaborating among the network. Supported this energy nodes will opt for the route in reliable.

C. Calculating hop-by-hop energy

When supply node sends request, nodes can check the energy of all its one hop neighbor nodes. Then the node choose consequent node that one has high energy value. All the nodes do an equivalent method.

D. Neighbor processing

This module is split into 2 sub modules named as 1) Poll method and information method

- Poll method

– By exploitation this module the node will verify the neighbors.

3.5. Data Process

In this sub module, the node ought to cross check the data. Ex, if node must verify the node x, then the champion checks the data (which is collected from the neighbor). throughout this checking methodology verifiers compares the house b/w each neighbor and node x. The distance is calculated in 2 ways in which

- Location based mostly comparison
- Data transmitted speed comparison

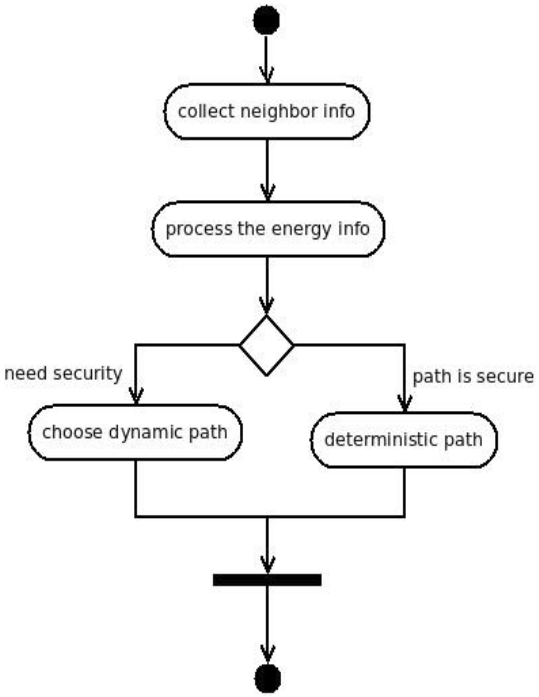


FIG.2: ACTIVITY OF PROPOSED MODEL

IV. RESULTS

To simulate our projected work we'd like Single computer with twenty GB disk area, 1GB RAM and software package is UNIX operating system OS (Ubuntu ten.04) and NS2.34. We have a tendency to use the programming languages: TCL, C++ (Optional). Fig. R1 shows the network placement.

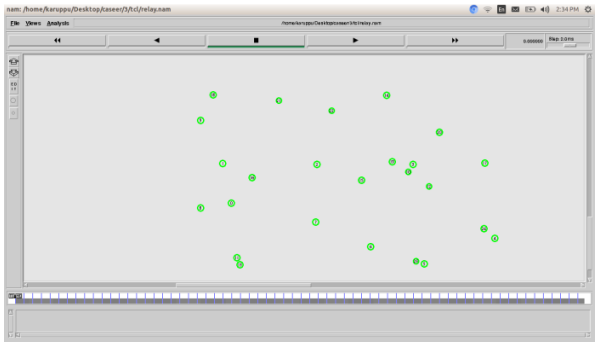


Fig.R1 network placement

Fig. R2 shows the results of route discovery.

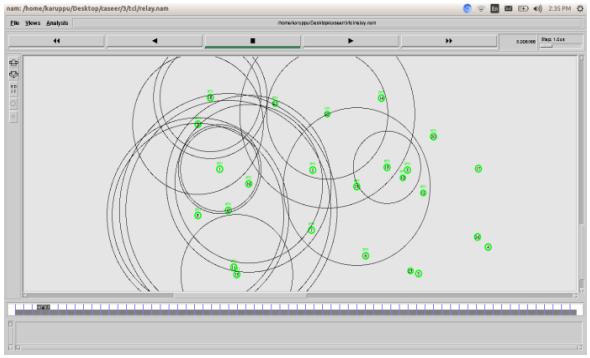
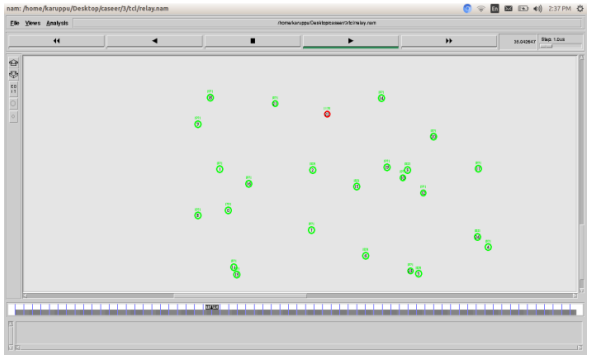


Fig.R2 route discovery

Fig. R3 shows the result of node failure



FigR3 node failure

Fig.R4 and R5 shows the attacker which is trying to track the source location

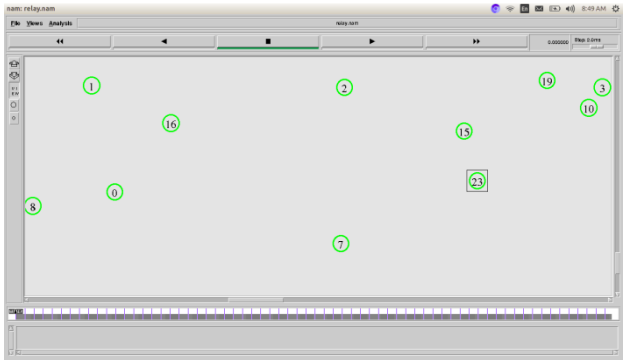


Fig.R4 attacker movement

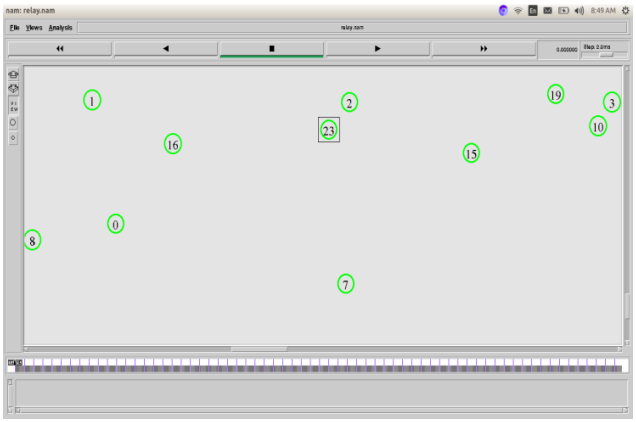


Fig.R5 attacker movement

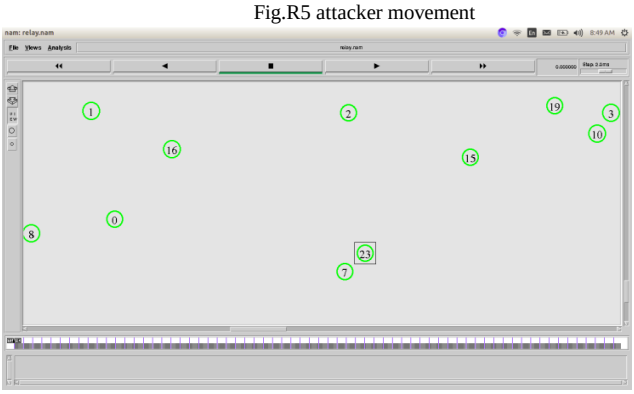


Fig.5 attacker fails to find the source

Fig.R6 shows the comparison of life time for existing, proposed and enhancement.

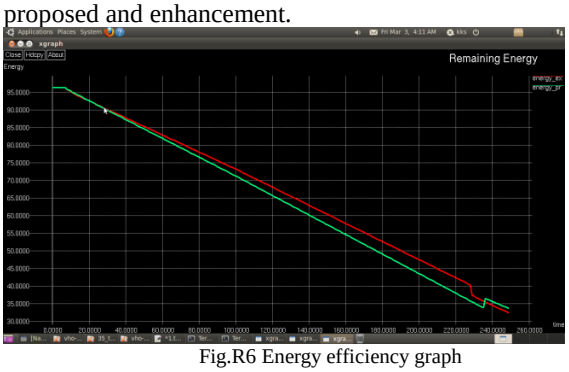


Fig.R6 Energy efficiency graph

The above fig R6 shows the energy efficiency comparison between the proposed method and existing method. Here green indicates proposed graph and whereas red indicates existing graph.

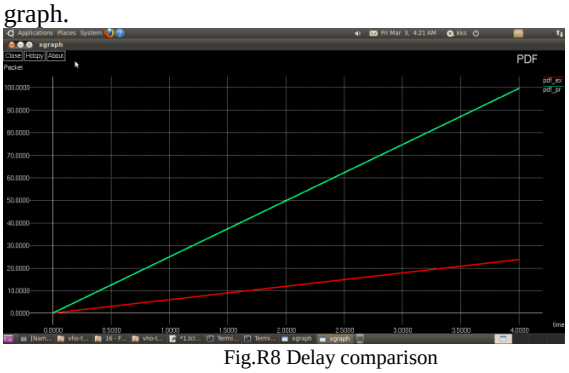


Fig.R8 Delay comparison

The above fig R8 shows the bar graph of delay comparison between proposed method and existing method. Green indicates proposed graph and where as red indicates existing graph.

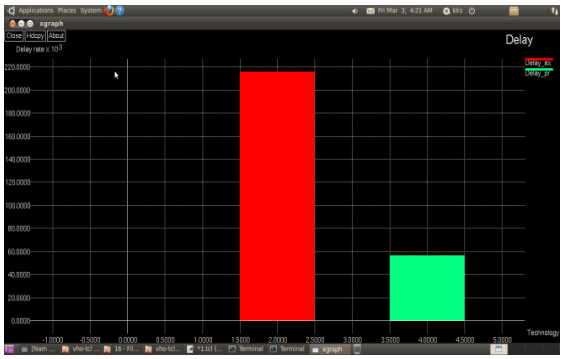


Fig.R7 shows the result of PDF comparison

The above fig R7 shows that power delivery ratio is more for proposed method compared to existing method.The green line indicates proposed graph and where as red line indicates the existing graph.

V. Conclusion

Here, it is presented an energy efficient Cost Aware secure Routing (CASER) protocol for WSNs to balance the energy consumption and increase network lifetime. CASER protocol is support multiple routing strategies in message forwarding to extend the lifetime and increasing routing security. Both theoretical analysis and simulation results provide that CASER has an excellent routing performance in terms of energy balance and routing path security. The CASER protocol provides a non-uniform energy deployment scheme to maximize the sensor network lifetime.

References

[1] Y. Huang, x. Yang, s. Yang, w. Yu, and x. Fu, “cross-layer approach asymmetry for wireless mesh access networks”, mar. 2011.

[2] V. Shah, e. Gelal, and p. Krishnamurthy, “handling asymmetry in power heterogeneous ad hoc networks: a cross layer approach”, Jul. 2007.

[3] J. Wu and f. Dai, “virtual backbone construction in MANET’s using adjustable transmission ranges”, sep. 2006.

[4] Optimized Retransmission Mechanism to Prevent Wastage of Spectrum in Seamless Mobility Handover Published in International Journal of Applied Engineering Research, ISSN 0973-4562 Vol. 10 No.5 (2015) pp. 3906-3910.(Indexed in Scopus)

[5] “Security in Wireless Sensor Networks: Key Management Module in EECBKM”Presented in International Conference on World Congress on Computing and Communication Technologies on Feb 27- & 28 and 1st march 2014, on St.Joseph college,Trichy.

[6] Survey of routing protocols in mobile ad-hoc network----> Kevin c. Lee, uichin lee and Mario gerla.

[7] S. Karthikeyan, S. Jayashri (2012), “Energy efficiency for heterogeneous wireless sensor networks”.