

A Survey on Energy Efficient Cost-Aware Routing Protocol for Wireless Sensor Networks

M. Venkata Nagi Reddy¹, M.Mazeed Ahamed², S.Karthikeyan³, V.G. Sivakumar⁴

^{1,2,3,4} Department of ECE, Sathyabama Institute of Science and Technology, Chennai, India

¹maramreddynagireddy@gmail.com, ²mazeedahamed@gmail.com, ³skarathi1879@gmail.com

Abstract-

A typical wireless sensor network consists of several tiny and low-power sensors which use radio frequencies to perform distributed sensing tasks. These nodes often have very limited and non-renewable energy resources, which makes energy as crucial design issue for these networks. Routing is another very important design issue for WSNs. A well designed routing protocol should balance the entire sensor network energy consumption along with high message delivery ratio and low energy consumption for message delivery, thereby extending the sensor network lifetime. So we have proposed the Active Trust technique is adopted to avoids black holes through the active creation a number of detection routes to quickly detect and obtain nodal trust and thus improve the data route security. In the trust management scheme, the trust model has two components: trust from direct observation and trust from indirect observation that proposed security in WSN. Finally we have proposed the Active Trust scheme fully uses residue energy to construct multiple detection routes. In this paper, we tend to propose a secure and efficient Cost-Aware Secure Routing (CASER) protocol which will address energy balance and routing security at the same time in WSNs. To enhance these project Hybrid cost ware secure routing algorithm implemented to proliferate lifetime of the network.

Keywords- Delivery Ratio, Efficiency, Energy Balance, Routing, security, Simulation.

I. INTRODUCTION

The basic concept of sensor network is to disperse tiny sensing devices; which have ability to sense the changes or developments of circumstances/parameters and correspond with other systems, over a prescribed area for some special purposes like environmental monitoring, surveillance, target tracking etc. Present sensors can supervise humidity, temperature, soil makeup, pressure, lighting conditions, vehicular movement, noise levels, the presence or absence of variety of substances or objects, mechanical stress and strain levels on related objects, and other parameters like Routing. WIRELESS ad hoc networks have been deployed at an increasingly fast rate, and are expected to reshape. Meanwhile, advances in hardware technology are constantly generating various wireless communication terminals to an shattering user population. In many scenarios, designs of wireless ad hoc network protocols are guided by two requirements - resilience to packet losses and energy efficiency. Discovering reliable routes can increase quality of the service. During the last decade, various routing

algorithms have been proposed focusing at prolonging reliability, energy-efficiency and the lifetime of wireless ad hoc networks. Effectively reduce the energy consumption of nodes and balance the traffic load among them in this work, CASER is proposed. This in turn saves energy as well and reduces the latency of packet delivery. To increase the network lifetime, power management and energy-efficient routing techniques become necessary.

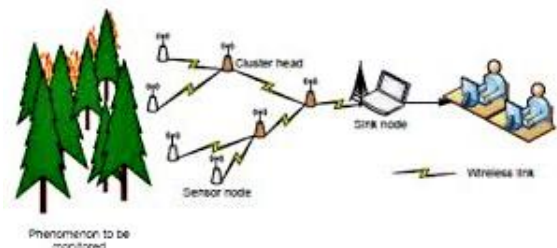


Fig 1: Architecture of typical WSN

II. LITERATURE SURVEY ANALYSIS:

A) F Richard Yu, Helen Tang², Shengrong Bu et al (2013), has outlined about Security and Quality of Service (Qos) Co-Design In Cooperative Mobile+ Ad Hoc Networks. In this paper he described that Qos can be

improved by cooperative communication in mobile adhoc Network (MANETs). Idea behind are single-antenna mobile nodes in a Multi user Scenario can share their antennas in a manner that creates a multiple-output (MIMO) system and virtual multiple- input. We introduce a game-theoretic approach to significantly evaluate the attack designs of the attacker so as to make a reasonable decision on relay selection and the authentication parameter adaptation to reach a understanding between security and QoS in CO-MANETs.

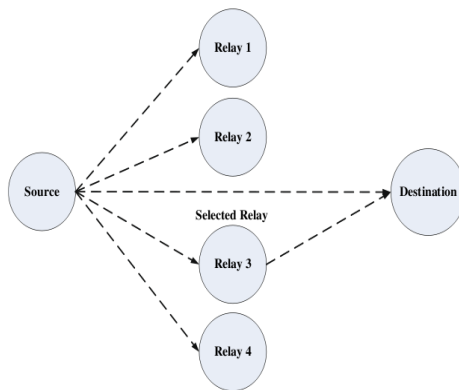


Fig 2: Multiple-output (MIMO) system

Advantages:

- Secure routing in Ad hoc networks.

Disadvantages:

- Single antennas with multi radio networks are traditionally create more traffic in the network.

B) Feng Li et al (2010),has outlined about Attack and Flee: Game-Theory-Based Analysis on Interactions among Nodes in MANETs. In this paper he described that in game theoretic scheme to analyze the strategy profiles for malicious and regular nodes. We model the direction as a dynamic Bayesian signaling game and consider and present underlining connection between nodes best combination of actions and gain of the individual strategy and the cost. Regular nodes restore their beliefs based on the opponents behavior, while malicious nodes analyze their risk of being caught to decide when to flee. Some possible remedies for regular nodes that can impact malicious nodes decisions are presented as well.

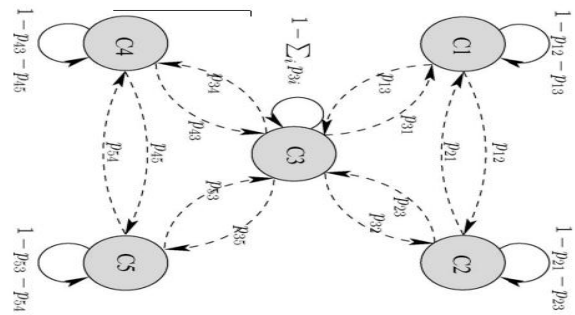


Fig 3: Interactions among Nodes in MANETs

Advantages:

- Calculate trust value more accursedly.

Disadvantages:

- We can observe only the single hop neighbours, it is not suitable for overall network.
- Overhead will be higher.

C) Shengrong Bu et al (2011),has investigated about Structural Results for Combined Continuous User Authentication and Intrusion Detection in High Security Mobile Ad-Hoc Networks. In this paper he described that A intrusion detection systems (IDSs) are also important in MANETs to effectively analyze malicious activities. Considering these two approaches jointly is effective in account system security requirements and optimal security design taking into resource constraints in MANETs. To gather the optimal scheme of combining continuous user authentication and IDSs in a distributed manner, we define the problem as a partially detectable Markov decision process (POMDP) multi-armed bandit problem. We present structural results method to solve the problem for a large network with a types of nodes. The policies defined from structural results are easy to implement in practical MANETs.

Advantages:

- Preventing hacker at the entry level checking.

Disadvantages:

- In this paper also we are using centralized nodes.
- Latency will be higher.

D) Pirzada et al (2006), has investigated about Routing based direct trust calculations. Here he described that Trust is a fractional value in $[0, 1]$. Performance of AODV and DSR protocol have been analyzed with the proposed trust scheme. On existing request and acknowledgement schemes in AODV and OLSR protocols. This local trust is precise.

Advantages:

- No single point failure.

Disadvantages:

- Additional hardware to monitor the packet drop/forward event of neighbours.

E) S. Buchegger et al (2004), C. Zouridaki et al (2005), has investigated about Past actions and present behavior are joined in Bayesian estimate to resolve trust. Trust is measured as probability value. The improvement of trust for several numbers of observations has been made.

Advantages

- No single point failure.

Disadvantages

- Observation collection and Bayesian calculations requires memory and computational complexity.

F) S.Karthikeyan, S.Jayashri et al(2012), 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.

Advantages:

- Easy to calculate the energy efficiency.
- Prolong the lifetime of the network.
- Network is re-energized

Existing method

Several geographical routing protocols are 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.

Draw backs:

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

III. PROPOSED METHOD

Basically in normal ad hoc network route selection will be select by source node only, in case any hacker can be enter the network in hidden way. It is too difficult to find. To solve these issue we proposed the packet delivery based Active Trust technique.

In the system with two observations one is direct and other one is indirect, in direct method each node can observe the behavior of other immediate nodes, and indirect model each node observes the information about multi-hop node by the immediate trustworthy node. By using the trust management scheme we can get the accurate value and we can avoid the misbehavior nodes from the route.

Advantages:

- Protect from the black hole attacks
- Secure level is high
- Boost up the Battery power

IV. CONCLUSION

In this paper, we conferred a secure and efficient Cost Aware secure Routing (CASER) protocol for WSNs to prolong network lifetime and balance the energy consumption. 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.

Acknowledgement

I am pleased to acknowledge my sincere thanks to Sathyabama Institute of Science and Technology, Chennai which has given a good platform to do my

survey work. I would also like to express my sincere thanks to my project guide S.Karthikeyan for providing me necessary support and details at right time during the progressive reviews.

REFERENCES

- [1] F Richard Yu, Helen Tang², Shengrong Bu (2013), "Security And Quality Of Service (Qos) Co-Design In Cooperative Mobile Ad Hoc Networks".
- [2] Feng Li (2010), "Attack and Flee: Game-Theory-Based Analysis on Interactions Among Nodes in MANETs".
- [3] Shengrong Bu (2011), "Structural Results for combined Continuous Intrusion Detection and User Authentication in High Security Mobile Ad-Hoc Networks".
- [4] Pirzada (2006), "Routing based direct trust calculations".
- [5] S. Buchegger(2004), C. Zouridaki (2005) , "Past actions and present behavior are combined in Bayesian estimate to determine trust".
- [6] S. Karthikeyan, S. Jayashri (2012), "Energy efficiency for heterogeneous wireless sensor networks".