INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

A COMPARITIVE STUDY ON COST AWARE SECURE ROUTING (CASER) PROTOCOL WITH SLEEP WAKE STATE ROUTING PROTOCOL (SWSR)

R.Sudha [1], G.Bakyalakshmi [2]

[1]Assistant Professor, Dept of CS, PSG College of Arts & Science, Coimbatore, Tamilnadu.
E-Mail: sudha279@yahoo.com
[2]Research scholar, Dept of CS, PSG College of Arts & Science, Coimbatore, Tamilnadu.
E-Mail:bakya.psg@gmail.com

Abstract: A wireless sensor network (WSN) of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. CASER tool is used to increase the life time of the networks. Caser tools use two parameters (i) energy balance control and (ii) probabilistic-based random walking. The EBC uses for energy consumption and the other one used for security. We propose non uniform technology in energy balanced consumption. In uniform technology the data's can't be send it for longer nodes to overcome this problem the non-uniform technology is proposed. Then we compared the Sleep awake protocol which is used to send the packet in energy efficient way

Keywords: Sensor networks, CASER, EBC, Protocols, Security

1. INTRODUCTION

A computer network or data network is a telecommunications network that allows computers to exchange data. In computer networks, networked computing devices pass data to each other along data connections. Data is transferred in the form of packets. The connections (network links) between nodes are established using either cable media or wireless media. The best-known computer network is the Internet. Network computer devices that originate, route and terminate the data are called network nodes. Nodes can include hosts such as personal computers, phones, servers as well as networking hardware. Two such devices are said to be networked together when one device is able to exchange information with the other device, whether or not they have a direct connection to each other.

The recent technological advances make wireless sensor networks (WSNs) technically and economically feasible to be widely used in both military and civilian applications, such as monitoring of ambient conditions related to the environment, precious species and critical infrastructures. A key feature of such networks is that each network consists of a large number of un-tethered and unattended sensor nodes. These nodes often have very limited and non-replenishable energy resources, which makes energy an important design issue for these networks.

Routing is another very challenging design issue for WSNs. A properly designed routing protocol should not only ensure high message delivery ratio and low energy consumption for message delivery, but also balance the entire sensor network energy consumption, and thereby extend the sensor network lifetime.

Routing is the process of selecting best paths in a network. A routing protocol specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network. Routing algorithms determine the specific choice of route. Each router has a priori knowledge only of networks attached to it directly. A routing protocol shares this information first among immediate neighbours, and then throughout the network.

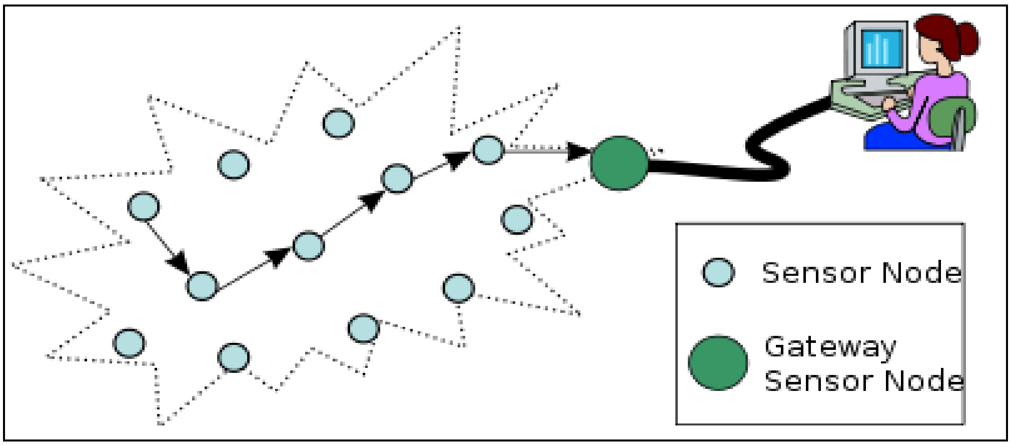

Fig. 1 wireless sensor network

The network router is quickly transforming from a device dedicated to connecting disparate networks to an integrated services device capable of multiple functions beyond routing. More Cisco customers are deploying integrated services routers sophisticated network routers that deliver voice, video, data and Internet access, wireless, and other applications.

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth.

2. RELATED WORK

2.1 Geographical forwarding problems: In our prior work we have considered a simple model where the number of relays is a constant which is known to the source. There the reward is simply the progress made by a relay node towards the sink. In the current work we have generalized our earlier model by allowing the number of relays to be not known to the source. Also, here we allow a general reward structure. There has been other work in the context of geographical forwarding and any cast routing, where the problem of choosing one among several neighboring nodes arises. Zorzi and Rao propose a distributed relaying algorithm called GeRaF (Geographical Random Forwarding) whose objective is to carry a packet to its destination in as few hops as possible, by making as large progress as possible at each relaying stage. These authors do not consider the trade-off between the relay selection delay and the reward gained by selecting a relay, which is a major contribution of our work. Liu et al. Propose a relay selection approach as a part of CMAC, a protocol for geographical packet forwarding. Under CMAC, node i chooses an r that minimizes the expected normalized latency (which is the average ratio0 of one-hop delay and progress). The Random Asynchronous Wakeup (RAW) protocol also considers transmitting to the first node to wake-up that makes a progress of greater than a threshold. Interestingly, this is the structure of the optimal policy for our simplified model. Thus we have provided analytical support for using such a threshold policy. For a sleep-wake cycling network, Kim et al. in have considered the problem of minimizing average end-to-end delay as a stochastic shortest path problem and have developed a distributed Bellman-Ford algorithm (referred to as the LOCAL-OPT) which yields optimal forwarding strategies for each node. However a major drawback is that a pre-configuration phase is required to run the LOCAL-OPT algorithm.

3. CASER PROTOCOL

CASER protocol has two major advantages: (i) It ensures balanced energy consumption of the entire sensor network so that the lifetime of the WSNs can be maximized. (ii) CASER protocol supports multiple routing strategies based on the routing requirements, including fast/slow message delivery and secure message delivery to prevent routing traceback attacks and malicious traffic jamming attacks in WSNs.

Our contributions of this paper can be summarized as follows:

1) We propose a secure and efficient Cost-Aware Secure Routing (CASER) protocol for WSNs. In this protocol, cost-aware based routing strategies can be applied to address the message delivery requirements.

2) We devise a quantitative scheme to balance the energy consumption so that both the sensor network lifetime and the total number of messages that can be delivered are maximized under the same energy deployment.

3) We develop theoretical formulas to estimate the number of routing hops in CASER under varying routing energy balance control and security requirements.

4) We quantitatively analyze security of the proposed routing algorithm.

5) We provide an optimal non-uniform energy deployment strategy for the given sensor networks based on the energy consumption ratio. Our theoretical and simulation results both show that under the same total energy deployment, we can increase the lifetime and the number of messages that can be delivered more than four times in the non-uniform energy deployment scenario.

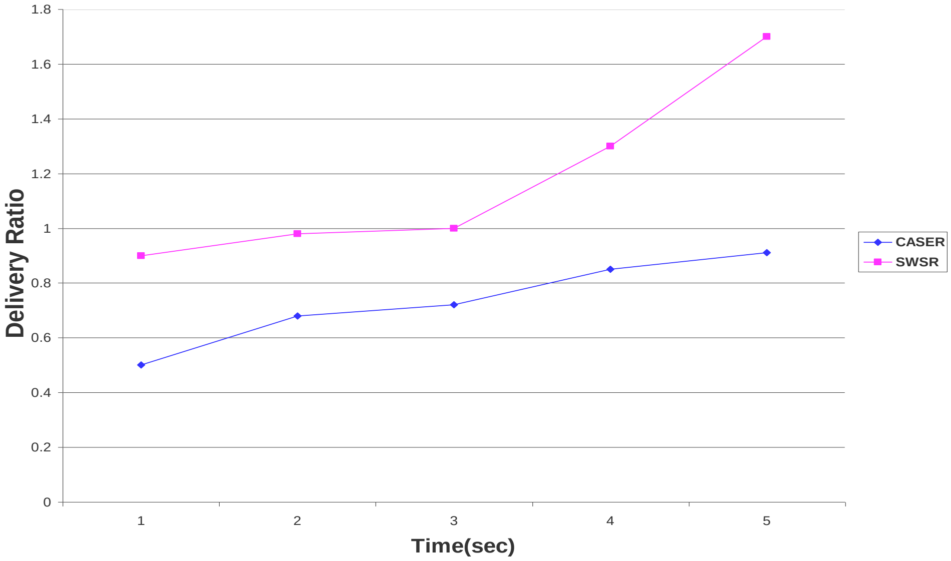

Fig.2 message delivery ratio

We summarize the CASER routing protocol in Algorithm1. It should be pointed out that the EBC parameter α can be configured in the message level, or in the node level based on the application scenario and the preference. When α increases from 0 to 1, more and more sensor nodes with relatively low energy levels will be excluded from the active routing selection. Therefore, the N_A^α shrinks as α increases. In other words, as α increases, the routing flexibility may reduce. As a result, the overall routing hops may increase. But since Ea(A) is defined as the average energy level of the nodes in NA, this subset is dynamic and will never be empty. Therefore, the next hop grid can always be selected from N_A^α.

Algorithm 1: Node A finds the next hop routing grid based on the EBC α€ 2 [0, 1]

(i) Compute the average remaining energy of the adjacent neighboring grids: Ea

$$\mathcal{E}_a(A) = \frac{1}{|\mathcal{N}_A|}\sum_{i\in\mathcal{N}_A}\mathcal{E}_{T_i}.$$

(ii) Determine the candidate grids for the next routing hop:

$$\mathcal{N}_A^{\alpha} = \{i \in \mathcal{N}_A \,|\, \mathcal{E}_{T_i} \geq \alpha\mathcal{E}_a(A)\}.$$

(iii) Send the message to the grid in the N$_A^\alpha$ that is closest to the sink node based on its relative location.

4. SLEEP-WAKE STATE ROUTING PROTOCOL

The high level design goal of SWS is to relax the assumption that every node knows the location of its first hop and second-hop neighbours, and to simplify the wake-up hardware and wakeup signal. Again considering SWS uses the following steps to wake up the guards along the route from *S* to *D*:

1. Node *S* broadcasts a wake-up signal to all its first-hop neighbors (*Z*,*W*,*n1*, □□*1*, □*1*). The wake-up signal includes the identity of both the current sender (*S*), the next-hop (*n1*), and the previous-hop (empty for *S*).

2. Each neighbors of *S*, after being woken up, decides whether to stay awake or go back to sleep based on the role that it may play on the ongoing communication. If that neighbor is the next-hop (*n1*), it stays awake to forward the data and to monitor the next-hop from it(*n2*). If that neighbor is a guard (□*1*, □*1*) for the next-hop *n1* over the link *n1*□*n2*, it stays awake to monitor the behavior of *n1*. If the node is a guard of a forwarding node over the previous-hop, it stays awake to detect fabrication by the forwarding node. A node can independently make this determination based on first and second-hop neighbor information. If none of these cases hold, the node goes back to sleep immediately.

3. Node *S* sends the data packet to *n1* following the timing schedule presented

4. Nodes *n1*, □*1*, and □*1* after being woken up continue to stay awake for *Tw*. After that, it goes back to sleep.

5. *n1* does the same steps that *S* did to wake up the next hop(*n2*), *n2*'s guards (□*2*, □*2*) and *n1*'s guards (*S*, □*1*, □*1*).

6. If *n1* fails to send the wakeup signal, the guard of *n1*with the lowest ID sends a two-hop broadcast of the wakeup signal through. If that guard fails, the guard with the next smallest ID sends the signal, and so on. This design ensures that if there is a chain of colluding malicious nodes then all the nodes will be suspected.

7. The process continues at each step till the destination. This scheme results in an increase in the energy consumption.

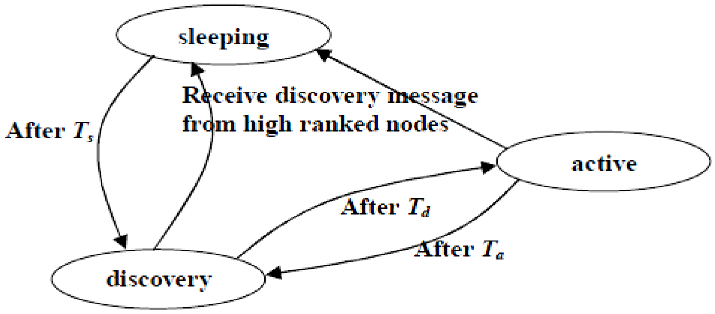

Fig.3 sleep wake state routing protocol

5. CONCLUSION

We are proposed and studied few protocols and compared the existing with proposed methods. The cost aware secure routing protocol is used to balance the energy consumption and increase network lifetime. Which is also having some drawbacks and it takes more time to send the data. So to overcome this problem we use sleep wake state routing protocol to send the packet in energy efficient way. In future work may be some efficient algorithm can be used to protect the data and send it in secure manner.

6. REFERENCES

[1] Y. Li, J. Ren, and J. Wu, “Quantitative measurement and design of source-location privacy schemes for wireless sensor networks,” IEEE Transactions on Parallel and Distributed Systems, accepted, to appear.

[2] Y. Li, J. Li, J. Ren, and J. Wu, “Providing hop-by-hop authentication and source privacy in wireless sensor networks,” in IEEE INFOCOM 2012 Mini-Conference, Orlando, Florida, USA., March 25-30, 2012 2012.

[3] B. Karp and H. T. Kung, “GPSR: Greedy perimeter stateless routing for wireless networks,” in MobiCom’2000, New York, NY, USA, 2000, pp. 243 – 254.

[4] J. Li, J. Jannotti, D. S. J. D. C. David, R. Karger, and R. Morris, “A scal- able location service fo geographic ad hoc routing,” in MobiCom’2000. ACM, 2000, pp. 120 – 130.

[5] Y. Xu, J. Heidemann, and D. Estrin, “Geography-informed energy conservation for ad-hoc routing,” in the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking, 2001, pp. 70–84.

[6] Y. Yu, R. Govindan, and D. Estrin, “Geographical and energy-aware routing: A recursive data dissemination protocol for wireless sensor networks,” UCLA Computer Science Department Technical Report, UCLACSD,May 2001.

[7] N. Bulusu, J. Heidemann, and D. Estrin, “Gps-less low cost outdoor localization for very small devices,” Computer science department, University of Southern California, Tech. Rep. Technical report00-729, April 2000.

[8] A. Savvides, C.-C. Han, and M. B. Srivastava, “Dynamic fine-grained localization in ad-hoc networks of sensors,” in Proceedings of the Seventh ACM Annual International Conference on Mobile Computing and Networking (MobiCom), July 2001, pp. 166–179.

[9] P. Bose, P. Morin, I. Stojmenovic, and J. Urrutia, “Routing with guaranteed delivery in adhoc wireless networks,” in 3rd Int. Workshopon Discrete Algorithms and methods for mobile computing and communications, 1999, pp. 48–55. 1045-9219 (c) 2013 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See

[10] “Routing with guaranteed delivery in ad hoc wireless networks,” in the 3rd ACM International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications (DIAL M 99), Seattle, WA, August 1999, pp. 48–55.