Secured Power Aware Routing Protocol (SPARP) for Wireless Sensor Networks

R. Prema
Assistant Professor
Department of Electronics
Karpagam University
Coimbatore – 641 021.

R. Rangarajan
Phd, Director
V.S.B. Engineering College
NH-67, Covai Road,
Karudayampalayam PO,
Karur – 639 111.

ABSTRACT

Several wireless sensor network applications ought to decide the intrinsic variance between energy efficient communication and the requirement to attain preferred quality of service (QoS) such as packet delivery ratio, delay and to reduce the power consumption of wireless sensor nodes. Also the intended protocols that are developed aims in providing better QoS with compromising security aspect. In order to address this challenge, we propose the Secured Power Aware Routing Protocol (PARP), which attains application-specified communication delays at low energy cost by dynamically adapting transmission power and routing decisions along with incorporating a novel cryptosystem. Through extensive simulation in NS2 the results prove that the proposed SPARP attains better QoS and reduced power consumption. Cryptool is used to test the novel proposed cryptosystem.

Keywords: Sensor networks, secured power aware routing, novel cryptosystem.

1. INTRODUCTION

Wireless Sensor Networks

Smart environments represent the next evolutionary development step in building, utilities, industrial, home, shipboard, and transportation systems automation. Like any sentient organism, the smart environment relies first and foremost on sensory data from the real world. Sensory data comes from multiple sensors of different modalities in distributed locations. The smart environment needs information about its surroundings as well as about its internal workings; this is captured in biological systems by the distinction between exteroceptors and proprioceptors.

The challenges in the hierarchy of: detecting the relevant quantities, monitoring and collecting the data, assessing and evaluating the information, formulating meaningful user displays, and performing decision-making and alarm functions are enormous. The information needed by smart environments is provided by Distributed Wireless Sensor Networks, which are responsible for sensing as well as for the first stages of the processing hierarchy. The importance of sensor networks is highlighted by the number of recent funding initiatives, including the DARPA SENSIT program, military programs, and NSF Program Announcements. Desirable functions for sensor nodes include: ease of installation, self-identification, self-diagnosis, reliability, time awareness for coordination with other nodes, some software functions and DSP, and standard control protocols and network interfaces.

This is an extension of our previous work [1]. In [1] we proposed power aware routing protocol for wireless sensor networks. In this paper we ought to propose an adaptive novel cryptosystem.

2. LITERATURE REVIEW

In [2], Chien-Yuan Chen, Cheng-Yuan Ku, and David C.Yen found ways to use the LLL algorithm to break the RSA system even when the value of d is large. According to their proposed cryptanalysis, if d satisfies $|X - d| < N0.25$, the RSA system will be possible to be resolved computationally.

In [3], R. Wattenhofer, L. Li, P. Bahl, and Y.-M. Wang proposed a topology control algorithm based on discretization of the coverage region of a node into cones. The idea is to select appropriate transmitter power levels to guarantee network connectivity while at the same time transmission energy is saved.

In [4], Y. Xu, J. Heidemann, and D. Estrin puts a node into sleep mode whenever its active collaboration in the current network task is not required is another way to save energy. The geographical adaptive fidelity (GAF) algorithm conserves energy by turning off nodes that are equivalent from a routing perspective, thereby keeping a constant level of routing fidelity.

In [5], C. Schurgers, V. Tsiatsis, S. Ganeriwal, and M. Srivastava utilise sparse topology and energy management (STEM) protocol which puts the nodes aggressively into sleep mode and only wakes them up when they are needed to forward data. Data fusion is a technique that can be used to reduce the amount of redundant information prevalent in dense sensor networks. By combining data with equal semantics, unnecessary power consumption due to transmission and processing of duplicate data is prevented.

In [6], Kwok-Wo Wong, Sun-Wah Ho, and Ching-Ki Yung, customized the chaotic cryptographic scheme to reduce the length of the ciphertext to a size slightly longer than that of the original message. Moreover, they introduced a session key in the cryptographic scheme so that the length of the ciphertext for a given message is not fixed.

In [7], Chang-Doo Lee, Bong-Jun Choi, and Kyoo-Seok Park proposed a block encryption algorithm, which is designed for each encryption key value to be applied to each round block with a different value. This algorithm needs a short processing time in encryption and decryption, has high intensity, and can be applied to electronic commerce and various applications of data protection.

In [8], L. Li, J. Y. Halpern, P. Bahl, Y.-M. Wang, and R. Wattenhofer proposed a topology control algorithm based on discretization of the coverage region of a node into cones. The

idea is to select appropriate transmitter power levels to guarantee network connectivity while at the same time transmission energy is saved.

In [9], Mark G. Simkin discusses five encryption techniques: transposition ciphers, cyclic substitution ciphers, Vigenere ciphers, exclusive OR ciphers, and permutation ciphers. Accompanying these discussions are explanations of how instructors can demonstrate these techniques with spreadsheet models.

In [10], Jun Wei, Xiaofeng Liao, Kwok-wo Wong, and Tao Xiang proposed a new chaotic cryptosystem. Instead of simply mixing the chaotic signal of the proposed chaotic cryptosystem with the ciphertext, a noise-like variable is utilized to govern the encryption and decryption processes. This adds statistical sense to the new cryptosystem.

In [11], Osama Mahmud Abu Abbas, Khalid Mohammad Nahar, and Mohammad Ahmad Tubishat, uses Arabic letters and their diacritics for encrypting English messages and vice versa. A pseudo random generator is used to generate integer numbers to represent each character in Arabic language. The same numbers are used again after sorting them to represent the English characters. The conclusions that extracted indicate the efficiency of ARAE system according to security and time performance.

Nevertheless, the diversities of all the above stated encryption methods, but all of them are common in some characteristic such as: The encryption operation can be implementing as a one to one relation, Usually there is a language redundancy problem, Semi random encryption methods, and Finding a way to cryptanalysis them is applicable, nevertheless, the needed time is.

3. Secured Power Aware Routing Protocol (SPARP) for Wireless Sensor Networks

3.1 Entropy:

The entropy defined as the amount of information in a message, and it is a function of the probability distribution over the set of all possible messages:

Let x1,…,xn are n possible messages occurring with probability p(x1),…,p(xn). Entropy of a given message is:

$$H(X) = -\sum_{i-1}^{n} p(X = x_i)\log_2 p(X = x_i)$$

..... (1)

Rate of language & Absolute Rate:

The average number of bits of information in each character

$$r = \frac{H(x)}{N}$$

,..... (2)

Where N is the length of the message is defined as a Rate of Language. In English language $1 \le r \le 1.5$

Absolute Rate is defined as the maximum number of bits of information that could be encoded in each character. If there are L characters in the language is:

$$R = \log_2 L$$

,..... (3)

For English language

$$R = \log_2 26$$

= 4.7 (bits/letter)

This means 25=32 combinations

The Redundancy of a language with rate r and absolute rate R is define by [8]:

D=R-r..... (4)

Applying above values gives:

D=4.7-1.5

=3.2

D/R*100=8%

Unicity Distance

The amount of ciphertext needed to uniquely determine the key:

If Hc(k) $\geq$ 0, then the cipher is unconditionally secure.

Unicity distance gives the number of characters required to uniquely determine the key, it does not indicate the computational difficulty of finding it, and given by [8]:

$$H_c(k) = \sum_k P_c(k)\log_2(1/P_c(k))$$

,.....

(5)

Modular Classes

If $x \equiv a(\mathrm{mod}\, n),$ then a, is called a residue of x modulo n. the residue classes of a modulo n, denoted by [a]n, is the set of all those integers that are congruent to a modulo n. that is [9]:

[a] n= {x: x ∈Z and $x \equiv a(\mathrm{mod}\, n)$ },.....(6)

= {a + k n: k ∈ Z}

As an example, let n=5, then there are five residue classes, module 5, namely the sets:

$$[0]_5 = \{ \Lambda \quad -5 \quad 0 \quad 5 \quad K \quad \}$$
$$[1]_5 = \{ K \quad -4 \quad 1 \quad 6 \quad K \quad \}$$
$$[2]_5 = \{ K \quad -3 \quad 2 \quad 7 \quad K \quad \}$$
$$[3]_5 = \{ K \quad -2 \quad 3 \quad 8 \quad K \quad \}$$
$$[4]_5 = \{ K \quad -1 \quad 4 \quad 9 \quad K \quad \}$$

The Novel Cryptosystem Methodology

The basic idea of our proposed cryptosystem method is depend on set theory. The encryption is defined as a relation between the language alphabetic and a set of sets "one set for each alphabetical element", while the decryption is a relation from a set of sets to the language alphabetic.

As an example for the set of sets is the set of residue classes for a given number N. Hence, the encryption process is defending a relation between the language alphabetic and the prime modular classes P for a given N integer number, where N>P, N is represent as a secret information between the sender and the reserve, which each of them agree on using a secret channelled. The sender uses our proposed encryption algorithm to send a message to the receiver, through

unsecured channel, and the receiver uses our proposed decryption algorithm to read the received message.

The encryption algorithm and the decryption algorithm are implemented in the next sub section for the English alphabetical language

Encryption algorithm

Input: Plaintext, N

Output: Cipher text

Process:

Step1: Find the modular classes for the input N

Step2: Apply each alphabetical English letter Li, to

a prime class Pi, 1=0,…25

Step3: For each input Plaintext letter Xj, randomly

select a number which belong to the

correspond classes.

Step4: Apply a permutation operation to the result

cipher text

Step5: End

Decryption algorithm

Input: Cipher Text, N

Output: Plaintext

Process:

Step1: Find the modular classes for the input N

Step2: Apply each alphabetical English letter Li, to

a prime class Pi, 1=0…25

Step3: Apply an inverse permutation operation to

the input cipher text

Step4: For each input Ciphertext letter Yj, find the

correspond class, that the digital number is

belong to.

Step5: End.

3.2. Power Aware Routing

3.2.1 Estimation of Link Quality

The communication in mobile ad-hoc network is based on electronic signals. In mobile ad-hoc networks it is possible that a communication path (route) will break. This will happen primarily because of the nodes present in the network are moving around the region. The fig.1, depicts the scenario when the link is active. In the fig.1, three nodes are present namely a, b and c. The node-b is within the range of the node-a and node-c. But, the node-a is not within the range of node-c and node-c is not within the range of node-a. Hence for transmission of data from node-a to node-c, the node-b acts as an intermediate node. After certain duration, due to the mobility of sensor nodes, the link gets break and the data communication between the nodes becomes unreliable.

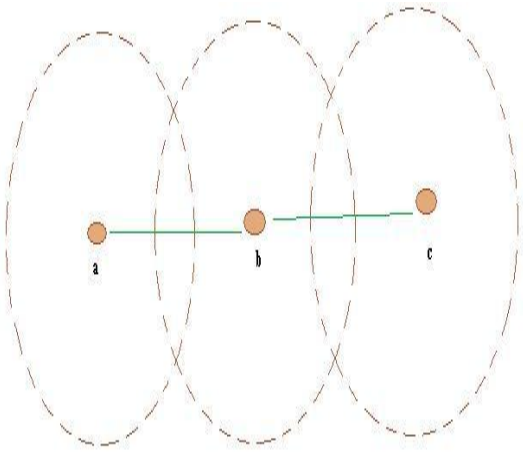

Fig.1 Before the link breaks

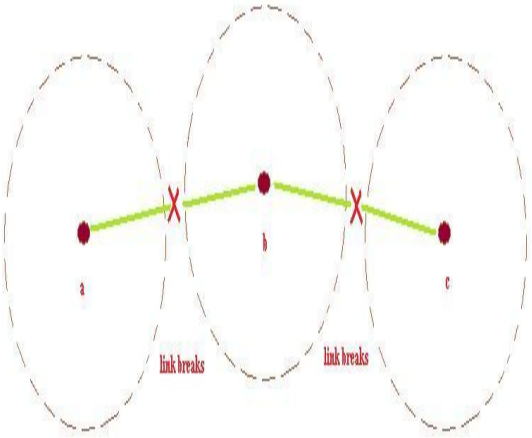

Fig.2 After the link breaks

Due to the mobility of nodes present in wireless sensor network it becomes mandatory to consider the quality of the link.

To be able to see that when a node in the wireless sensor network is moving and hence a route is about to break. So that factor, it is probable to measure the quality of the signal and based upon that presumption, when the link is going to break. This information which is identified by the physical layer is send to the upper layer when packets are received from a node, and then indicate that node is in pre-emptive zone. Pre-emptive zone is the region where the signal strength is weaker which leads to the link failure. Pre-emptive zone uses the pre-emptive threshold value to fix the pr-emptive zone's location. Thus, using the received signal strength from physical layer, the quality of the link is predicted and then the links which are having low signal strength will be discarded from the route selection.

When a sending node broadcasts RTS packet, it piggybacks its transmission power. While receiving the RTS packet, the projected node quantifies the strength of the signal received.

$P_R = P_T (\lambda / 4 \prod d)^2 * (UG_T) * (UG_R)$

Hence,

$L_q = P_R$

Where,

P_R refers Power of the Receiving node,

P_T stands for Power of the Transmitting node,

λ stands for wavelength carrier,

d is the distance between the sending and the receiving node,

UG_R stands for unity gain of receiving omni-directional antenna

UG_T stands for unity gain of transmitting omni-directional antenna.

$RN = \max (L_{q\,\&}\ R_{POW})$

Where,

CV = Cost Value,

L_q = Link quality

R_{POW} = Residual Power of the sensor node

In the proposed work Power Aware Routing Protocol (PARP) a cost value (CV) is calculated. CV is computed based on the on the quality of the link of each wireless sensor node. Among all the sensor nodes in the network, there are some robust nodes. These robust nodes serve as the backbone for the routing in wireless sensor networks. The remaining sensor nodes are common sensor nodes. Each robust node maintains a table of sensor node power at other robust nodes. So in the route, each robust node will compute the end-to-end power from itself to any other robust nodes. The sensor node power is estimated and updated periodically by each robust node. The robust node which is nearest to the source node finds the robust nodes which are along the route towards destination sensor node. Then packets will be forwarded through these robust nodes to the destination node. Since robust nodes have better communication capability than common nodes, most of the time the power is less than the maximum power.

3.2.2. Working Mechanism of PARP

1. Each robust node can arrive at nearby robust nodes directly. When a robust node goes out of a grid, it initiates a robust node election process in the grid and a new robust node will be selected.
2. Each Robust node holds a table of node power. Each Robust node can calculate the end-to-end power from itself to any other robust nodes. The node delay is estimated and updated periodically by each robust node.
3. In case a source node S needs to setup a route to a destination D. It is considered by the case where the source node S itself is a robust node. In this case, first the robust node S needs to know about the current location of the destination node D. With the information of D's location, S knows about the grid Ld where D stays, and the Robust node Ltd in the grid Ld.
4. Then S calculates the minimum power between S and Ltd by means of the power table, and also discovers the route with the minimum power. If the minimum power is greater than the required power, then the route can not be established. The source sensor node generates a unique req_id for each route request. When an intermediate node obtains the REQ packet, it adds the powers of the incoming link and itself to t_power, and compares the updated t_power with the max_power. If t_power is less than the max_power, it adds up itself to the route_list, and forwards the REQ packet to the neighbors. If t_power is greater than max_power, the node will drop the REQ packet.
5. If the minimum power between S and Ltd is less than the maximum power, sensor node S will notify Ltd to locate a route to the destination D. Then Ltd will update the t_power by adding the power between Ltd and D. If the updated t_power is less than max_power, a valid route is found. Ltd will send an ACK (acknowledge) packet to S along the reverse path to ascertain that the route is setup. And each node in the route will updates its node power. After that S can start sending data.
6. If S is not a Robust node, then S will first discover a path to the nearby Robust node with less power than required. Node S sends out the route request (REQ) packet by flooding to all the sensor nodes in its grid. Only sensor nodes in the same grid will process and forward the REQ packet. When a node gets the REQ packet, it will update the power from source to their locations (t_power). If t_power is less than max_power, it adds itself to the route_list, and forwards the REQ packet to the neighbors. If t_power is larger than max_power, the node will drop the REQ packet. When the Robust node in this grid gets the first REQ packet, it also updates the t_power and compares it with max_power. If t_power is less than max_power, it will calculate the minimum power between itself and the robust node which is nearest to the destination. The remaining steps are the same as above.
7. Sensor node power and current location information of robust nodes has to be updated and distributed among all robust nodes. The distribution is done periodically, and the length of the updating period depends on the network dynamics, such as sensor node mobility, sensor network traffic, sensor node communication capability, etc.

3.2.3 Election of robust node

At the start, one robust node is set in each grid. We need an election mechanism to produce new Robust nodes because robust nodes also move around. When a Robust node leaves its current grid or due to any other reason there is no robust node in the grid. Suppose, there are more Robust nodes in the current grid of the network, then, the next node with least weighted value from the sorted list will be chosen as the new Robust node for the grid. In the proposed routing algorithm, we need to compute the minimum delay between two robust nodes, and find the path with the minimum delay.

For each valid path Pi,

For every node nk in Pi

t_power = t_power + power (nL, nk) + power (nk)

If t_power >= max_power, delete this path, break.

If t_power >= min_power, delete this path, break.

If nk is the destination D, and t_power< min_power, min_power = t_power;

best_path = Pi + {nk};

Else add node nk to the end of the path,

End For

End For

Pseudo code for Robust Sensor node election

4. SIMULATION SETTINGS, PERFORMANCE METRICS

4.1. Simulation settings

Table 1. Simulation settings

No. of Nodes	50, 75, 100, 125 and 150
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512 KB
Mobility Model	Random Way Point
Speed	5 m/s
Pause time	100 Seconds

4.2. Performance Metrics

Average end-to-end delay: The end-to-end-delay is averaged over all surviving data packets from the source sensor node to the destination sensor node.

Average Packet Delivery Ratio: It is the ratio of the number of packets received successfully and the total number of packets sent.

Total power consumption: It is the average power consumption of all the sensor nodes in the network.

5. RESULTS

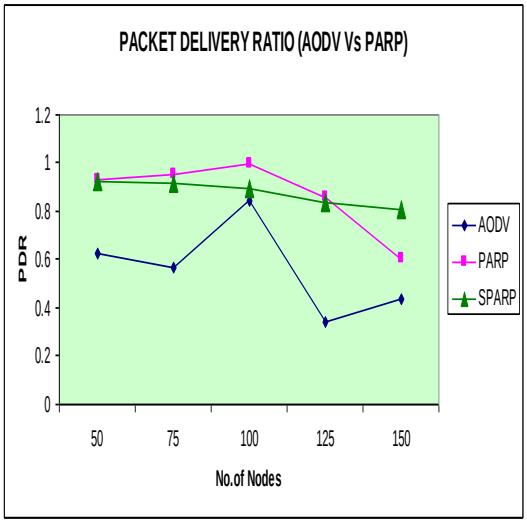

Fig.3 No.of Nodes Vs Packet Delivery Ratio

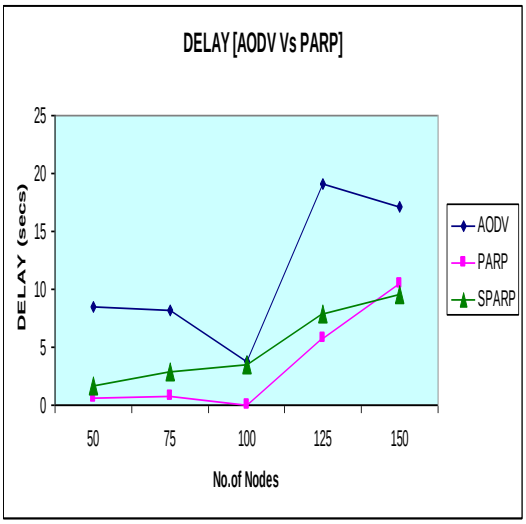

Fig.4 No.of Nodes Vs Delay

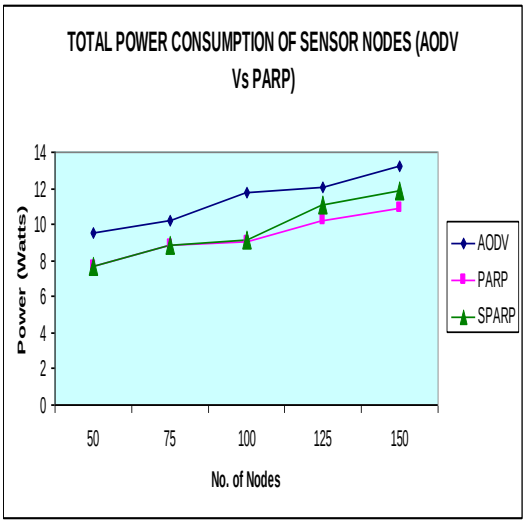

Fig.5 No.of Nodes Vs Total Power Consumption

6. CONCLUSION

In this paper in order to attain preferred quality of service (QoS) such as packet delivery ratio, delay and to reduce the power consumption of wireless sensor nodes we proposed secured power aware routing protocol (SPARP), which attains application-specified communication delays at low energy cost by dynamically adapting transmission power and routing decisions along with incorporating a novel cryptosystem. Through extensive simulation in NS2 the results proved that the proposed SPARP attains better QoS and reduced power consumption. For security validation Cryptool is used to test the novel proposed cryptosystem.

7. REFERENCES

[1] R. Prema and R. Rangarajan, "Power Aware Routing Protocol (PARP) for Wireless Sensor Networks," Wireless Sensor Network, Vol. 4 No. 5, 2012, pp. 133-137.

[2] Chien-Yuan Chen, Cheng-Yuan Ku b and David C.Yen, "Cryptanalysis of large RSA exponent by using the LLL algorithm", in Proceedings of The Tenth National Conference on Information Security, Taiwan, Pages: 45-50, 2000.

[3] R. Wattenhofer, L. Li, P. Bahl, and Y.-M. Wang. Distributed topology control for power efficient operation in multihop wireless ad hoc networks. In Proc. IEEE INFOCOM, pages 1388–1397, Apr. 2001.

[4] Y. Xu, J. Heidemann, and D. Estrin. Geography-informed energy conservation for ad hoc routing. In Proc. ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), pages 70–84, July 2001.

[5] C. Schurgers, V. Tsiatsis, S. Ganeriwal, and M. Srivastava. Topology management for sensor networks: Exploiting latency and density. In Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), pages 135–145, June 2002.

[6] Kwok-Wo Wong, Sun-Wah Ho, and Ching-Ki Yung, "A chaotic cryptography scheme for generating short ciphertext", Physics Letters A, Volume 310, Number 1, Pages:67-73, 2003.

[7] Chang-Doo Lee, Bong-Jun Choi and Kyoo-Seok Park, "Design and evaluation of a block encryption algorithm using dynamic-key mechanism". Future Generation Computer Systems, Volume: 20, Issue: 2, Pages: 327 - 338, 2004.

[8] L. Li, J. Y. Halpern, P. Bahl, Y.-M. Wang, and R. Wattenhofer. A cone-based distributed topology-control algorithm for wireless multi-hop networks. IEEE/ACM Transactions on Networking, 13(1):147–159, Feb. 2005.

[9] Mark G. Simkin, "Using Spreadsheets to Teach Data Encryption Techniques", AIS Educator Association, Volume 1, Number 1, pages 27 - 37, 2006.

[10] Jun Wei, Xiaofeng Liao, Kwok-wo Wong, and Tao Xiang, "A new chaotic cryptosystem", Chaos Solitons & Fractals 30 (5): 1143-1152 Dec 2006.

[11] Osama Mahmud Abu Abbas, Khalid Mohammad Nahar, and Mohammad Ahmad Tubishat, "Arae Cipher System", Computer Science Department, IT Faculty, Yarmouk University, Jordan, 2007.