Energy Efficient Routing and Secure Data Communication in Wireless Sensor Networks

Kamanashis Biswas, Vallipuram Muthukkumarasamy, Elankayer Sithirasenan, Kalvinder Singh
Griffith University, Gold Coast, Australia
kamanashis.biswas@griffithuni.edu.au
{v.muthu, e.sithirasenan}@griffith.edu.au
kalsingh@au.ibm.com

Abstract. About 70% of the total energy is dissipated for data transmission in most of the Wireless Sensor Network (WSN) applications. Hence, energy aware routing protocols are required to find efficient route in order to prolong the network lifetime in WSNs. Security is another critical issue in WSNs and a number of security schemes are developed to provide security services. However, these algorithms have their own weaknesses, such as vulnerable to chosen-plaintext attack, brute force attack and computational complexity. In this study, we propose an energy aware heuristic-based routing protocol and a lightweight cryptographic scheme to provide energy efficiency and security in WSNs. Our further aim is to design secure multi-path routing and DNA-based cryptographic schemes for WSNs.

1 Introduction

Wireless sensor networks consist of thousands of tiny sensor nodes (SNs) which monitor temperature, humidity, motions and sound. These nodes regularly send collected data to the base station (BS) via integrated radio transmitter. The key challenge in WSNs is to prolong the lifetime of SNs since it is not possible to recharge the batteries of SNs. Therefore, energy efficient mechanisms are required for computational operations of nodes and communication protocols. Security is another challenging issue in WSNs because SNs are usually deployed in hostile environments and vulnerable to many security attacks. Hence, WSNs need efficient encryption schemes in terms of operation speed, storage and power consumption. We aim to address the following research questions in our study.

1. How to design energy efficient location-based routing protocol using heuristic function to prolong network lifetime?
2. How can we design lightweight and secure cryptosystems using ECC and DNA-based mechanisms to provide authentication and data confidentiality?
3. What are the effective ways to tightly couple security mechanisms with core routing protocols to establish a secure communication channel between participating nodes?
2 Energy Aware Heuristic-based Routing Protocol

We assume that every SN is assigned a unique node ID and every SN knows the location of BS as well as its own. We use the same radio communication model as reported in [1].

2.1 The Proposed EAHR Protocol

Heuristic Function and A* Search Algorithm: The heuristic function provides a good estimate of how far the destination node from the current node and thus helps to guide the search procedure. The EAHR protocol uses the following heuristic function: \( f(n) = h(n) + g(n) + \frac{(A/(3\sqrt{3}R_s^2))/\text{Eng}(n)}{2} \), where, \( f(n) \) denotes heuristic value of node \( n \), \( h(n) \) is the estimated cost from node \( n \) to BS and \( g(n) \) is cost so far. \( A \) is the deployment area, \( R_s \) is the radio range of sensor nodes and \( \text{Eng}(n) \) denotes the energy level of node \( n \).

A* uses best-first-search technique to find the path that appears to be most likely to lead towards the goal on the basis of heuristic function. The available node with the smallest value of \( f \) is the node that should be expanded next.

Routing Procedure: Let us consider the network topology shown in Fig. 1. Suppose, node 12 has to find a route to the BS and the initial parameters are: \{[g(10) = 3, g(11) = 1.5]; [h(10) = 10, h(11) = 10.5]; [\text{Eng}(10) = \text{Eng}(11) = 0.5]\}; threshold level = 0.25. Hence, we get the following \( f \) values for node 10 and 11: \{f(10) = 13 and f(11) = 12\}. Since the \( f \) value of node 11 is smaller than that of node 10, node 12 selects node 11 as forwarding node. However, during next hop selection process, the algorithm computes the \( f \) value for node 9 via both node 10 and 11. Let us say, the \( f \) value to reach node 9 is 12 through node 10 and 12.5 through node 11. Since, the route via node 10 is shorter than the previous route, node 12 updates its routing table according to new route information. In this way, node 12 finds the optimal route to the BS using A* search algorithm.

Suppose, after time \( t \), the energy level of node 10 and 11 degrades to 0.2 (below threshold level) and 0.4 joules respectively. At this stage, node 12 recomputes the \( f \) value of node 10 i.e., \( f(10) = 3 + 10 + 4.27/0.2 = 34.35 \). Since the value is greater than that of node 11 (\( f(11) = 12 \)), node 11 is selected as the forwarding node by node 12.

![Fig. 1. Example of EAHR topology](image-url)
2.2 Experiments and Analysis
We simulated our proposed EAHR algorithm in OMNET++ and compared the results with WSNHA-GAHR protocol [2]. We randomly deploy 25 nodes (with initial energy 0.35J) in 50 × 50 \( (m^2) \) simulation area. Fig. 2 shows that our proposed EAHR protocol performs better than GAHR protocol in terms of network lifetime, energy usage, throughput and network partition.

3 The Proposed Encryption Scheme
Our proposed scheme is divided into two phases: pseudorandom bit sequence generation phase and encryption phase. Here, we describe the protocol in detail.

**Generation of Pseudorandom Bit Sequence:** At this phase, each SN generates a large number of keys using elliptic curve operations. When a node has to send data packets, it randomly selects a key from the key pool and converts it into hash code using a hash function. This code is shared with the destination node. The destination node retrieves the shared key and sends the hash code of immediate next key of the shared key. This secret key is used in N-logistic-tent map to generate random bit sequence in our proposed scheme [3].

**The Encryption Procedure:** At first, we divide the random bit sequence into two blocks of 64-bits and the first block is further subdivided into chunk of 8-bits. Then, we calculate the number of 1’s in each byte and the sum of 1’s for each consecutive 4 bytes block. After that, we convert the plaintext to binary code by mapping the characters into their corresponding ASCII codes. The first genetic operation i.e., mutation is performed on each byte of plaintext using the total number of 1’s as the starting index of the mutation process. The mutated...
plaintext is then crossovered with random bit sequence as shown in the Fig. 3. Finally, the crossovered plaintext is xor-ed with second block of random bit sequence to generate the ciphertext. The decryption process is simply reverse of the encryption procedure.

Security and Performance Analysis: We tested our proposed scheme against brute force attack, statistical analysis attack, related-key attack, timing attack and chosen plaintext attack. Experimental results show that these attacks are not fruitful due to frequent re-keying and data independent behavioural characteristics of ciphertext. We also implemented our encryption scheme in Mica2 sensor mote and compared the results with AES and SkipJack protocols.

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>CPU Cycles</th>
<th>Time (ms)</th>
<th>RAM Usage (bytes)</th>
<th>ROM Usage (bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SkipJack</td>
<td>91224</td>
<td>12.353</td>
<td>7218</td>
<td>292</td>
</tr>
<tr>
<td>AES</td>
<td>68512</td>
<td>9.287</td>
<td>6994</td>
<td>324</td>
</tr>
<tr>
<td>Proposed</td>
<td>56124</td>
<td>7.579</td>
<td>5020</td>
<td>216</td>
</tr>
</tbody>
</table>

4 Future Work
Our future plan is to develop a trust and reputation management system to monitor the behaviour of nodes and identify security attacks in advance. We also plan to design and implement secure multi-path routing algorithms and DNA-based cryptographic schemes for WSNs.

References