Secure Energy Saving And Reliability Of Events In Wireless Sensor Networks

Vijay Udagatti
M Tech Student
Department of C S E
VTU, J.N.N.College of Engineering, Karnataka, India

Abstract— **This paper deals with a novel forwarding scheme for wireless sensor networks aimed at combining low computational complexity and high performance in terms of energy efficiency and reliability. The proposed approach relies on a packet-splitting algorithm based on the Chinese Remainder Theorem (CRT) and is characterized by a simple modular division between integers. In addition to CRT method for packet splitting, we also propose a efficient method for packet routing such that the forwarding the split packets to the base station. Though simulation we prove that the proposed method is secure and also energy efficient with increased reliability.**

Keywords: **security; Chinese remainder theorem, random propagation**

I. INTRODUCTION

A WIRELESS sensor network (WSN) is composed of a large number of low-cost devices distributed over a geographic area. Sensor nodes have limited processing capabilities, therefore a simplified protocol architecture should be designed so as to make communications simple and efficient. Moreover, usually the power supply unit is based on an energy-limited battery; therefore solutions elaborated for these networks should be aimed at minimizing the energy consumption. To this purpose, several works have shown that energy consumption is mainly due to data transmission, and accordingly energy conservation schemes have been proposed aimed at minimizing the energy consumption of the radio interface.

With the aim of reducing energy consumption while taking the algorithmic complexity into account, authors in [1] proposed a novel approach that splits the original messages into several packets such that each node in the network will forward only small subpackets. The splitting procedure is achieved applying the Chinese Remainder Theorem (CRT) algorithm [2], which is characterized by a simple modular division between integers. The sink node, once all subpackets (called CRT components) are received correctly, will recombine them, thus original message. The splitting procedure is especially helpful for those forwarding nodes that are more solicited than others due to their position inside the network. Regarding the complexity, in the proposed approach, almost all nodes operate as in a classical forwarding algorithm and, with the exception of the sink, a few low-complex arithmetic operations are needed. If we consider that the sink node is computationally and energetically more equipped than the other sensor nodes, the overall complexity remains low and suitable for a WSN. But this technique is not secure enough. Same routing path is used, so an attacker can easily capture the CRT packets and reassemble them. Also the chance of routing path being same is high, so packets may be lost due to sudden congestion in the work. In this paper, we propose solution to handle this problem and still the core of energy saving and increased reliability is maintained along with secure routing scheme so attacker is not able to receive all CRT packets and also no packets are lost due to sudden congestion.

The rest of the paper is organized as follows. Section II presents a brief summary of related works already existing in literature and highlights the distinguished approach of our solution as compared to them. Section III describes the overview of the proposed solution Section IV describes the proposed solution in detail. In Section V, describes the performance of the proposed solution. Finally, in Section VI, some concluding remarks are drawn.

II. RELATED WORK

Energy saving, reliability, and security of data are three key issues in WSNs.

With regards to energy saving, two main approaches can be found in the literature: duty cycling and in-network aggregation; see [3] and [4], respectively. The first approach consists in putting the radio transceiver on sleep mode (also known as power-saving mode) whenever communication is not needed. Although this is the most effective way to reduce energy consumption,

a sleep/wakeup scheduling algorithm is required (which implies solving critical synchronization issues), and energy saving is obtained at the expense of an increased node complexity and network latency. The second approach is intended to merge routing and data aggregation techniques and is primarily aimed at reducing the number of transmissions. In this perspective, and in the specific target to improve robustness of data aggregation, multipath routing algorithms together with erasure codes can be employed. However, the most commonly used erasure codes are not suitable for WSNs.

An interesting example of using a multipath approach together with erasure codes to increase the reliability of a WSN has been proposed in [5]. However, in that work, the authors suggested the use of disjoint paths. When compared to our proposed forwarding technique, using disjoint paths has two main drawbacks. First, a route discovery mechanism is needed. Second, as the numbers of disjoint paths are limited, the numbers of splits (and therefore the achievable energy reduction factor) are limited as well. Furthermore, in [5], the authors considered general forward error correction (FEC) techniques without investigating their specific complexities and/or their impact on energy consumption.

Another similar work is [6], where the authors have proposed a protocol called ReInForM (Reliable Information Forwarding using Multiple paths in sensor networks). The main idea investigated in this paper is the introduction of redundancy in data to increase the probability of data delivery. The redundancy adopted is in the form of multiple copies of the same packet that travel to the destination along multiple paths. However, as shown in [7], multiple paths could remarkably consume more energy than the single shortest path because several copies of the same packet have to be sent. Furthermore, in all the papers mentioned, the authors do not consider the splitting procedure as a method for reducing energy consumption. An attempt to guarantee reliability, while minimizing the energy consumption and, at the same time, considering a packet-splitting procedure, has been made in [8]. As in [5], the authors use distinct paths and erasure codes to provide reliability in the network. However, the algorithm proposed is a centralized one based on convex programming that is not suitable for WSNs.

III. OVERVIEW OF PROPOSED SOLUTION

Our proposed solution consists of 3 stages.

1. Split packets with CRT
2. Randomly propagate the CRT towards the base station
3. Reassemble the packets to form the original data.

The third stage follows the first two stages are as proposed in [1].

The node which generates the data split the packets according the CRT method. The split packets are not routed directly to the base station using traditional routing. In this project we propose a mechanism to forward the packets to the destination using a unique forwarding mechanism such that the route is not predictable.

By using unpredictable routes we are securing the packets from the attacker, so that he will not be able to eavesdrop the packets.

Once the CRT packets are received at the sink, sink re assemble the original data from the CRT packets received.

IV. DETAILS OF PROPOSED SECURITY MECHANISM

A. CRT Packet splitting

When a node generates the data, it split into many subpackets using the CRT algorithm.

The Chinese Reminder Theorem is an ancient but important calculation algorithm in modular arithmetic. The Chinese Remainder Theorem enables one to solve simultaneous equations with respect to different moduli in considerable generality

The Chinese Remainder Theorem says that certain systems of simultaneous congruences with different moduli have solutions.

The theorem can be written mathematically as follows

Let **r** and **s** be positive integers which are relatively prime and let **a** and **b** be any two integers. Then there is an integer **N** such that

$$N \equiv a \pmod{r} \qquad (1)$$

and

$$N \equiv b \pmod{s} \qquad (2)$$

Moreover, **N** is uniquely determined modulo **r s**. An equivalent statement is that if **(r, s) =1**, then every pair of residue classes modulo **r** and **s** corresponds to a simple residue class modulo **r s**.

By using the concept of Chinese remainder theorem the input data is broken to many smaller numbers. Each is encoded as packet.

B. Routing of Packets

If the Routing becomes predictable the attackers can eavesdrop and collect the CRT packets to find

the original data. Sending the each CRT packet in diverse path is a solution to provide security but it will be result in loss of energy. So we a solution which is both secure and energy optimal.

A node on generating the CRT packets must employ random till some hops and then continue routing all CRT packets in the same path.

In the proposed algorithm, each node maintains a count of how many times it has chosen the next hop neighbor for forwarding.

The forwarding consists of two stages

1. Random propagation phase
2. Routing Phase

After the packets are split, the node initializes with packet with a hop count value. This value will decide the number of times the packet has to be randomly propagated.

The node will chose a neighbor node whose forward count in the neighbor forward table is less and forward the packet to that neighbor node. The hop count is reduced by 1. The next node also does in the same way. Once the hop count is 0, the node will forward using the routing process to the base station. Route can be constructed and kept using DSR at the initialization time of the network.

The hop count value will decide how long random propagation needs to be done. There are two advantages with this approach. It is difficult for the attacker to know the path of the routing. Also the propagation is done to the nodes whose forwarding count is less, thereby the low energy node is chosen to forward data.

V. PERFORMANCE ANALYSIS

In this section, we compare the performance of proposed algorithm in terms of energy consumption to those obtained by SP. Moreover, we provide some results obtained comparing the proposed to the most naive splitting scheme, a simple packet division into chunks. The results have been obtained through NS2 simulator [9]. We first show a comparison between the results obtained through the analysis and those obtained through the simulator. Then, we analyze some other parameters in order to show the advantages of the proposed technique.

From the performance graph we see that the packet interception probability is higher in the CRT approach compared to our approach.

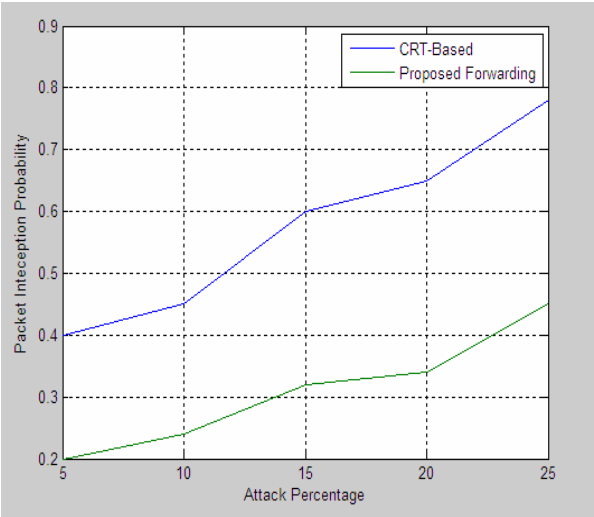

Fig 1: packet interception probability

From the performance analysis for providing additional security the cost incurred in terms of energy is only slightly higher than CRT based solution.

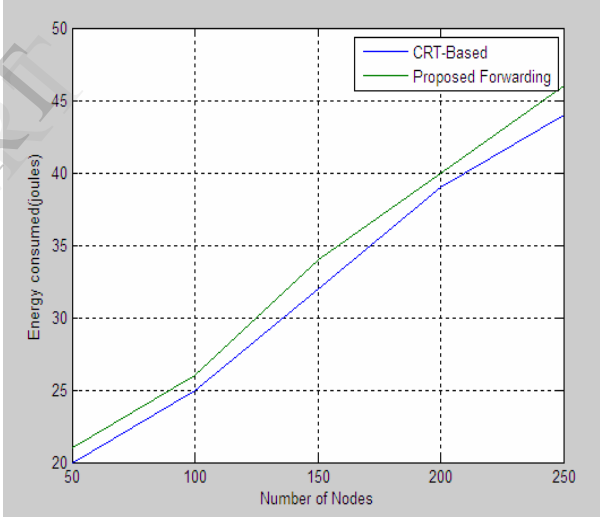

Fig 1: packet interception probability

VI. CONCLUSION

In this paper, we have detailed proposed solution to securely transmit the data in the sensor network. The proposed approach is safe against attackers, energy saving and also reliable. Through simulation we have proved the energy consumption in our solution is comparatively less than the existing solutions.

When any one of CRT packets are lost, it is difficult to construct the original packets at the base station. It needs to ask for retransmission. Our future work will address this challenge to avoid retransmission.

REFERENCES

[1] Giuseppe Campobello, Alessandro Leonardi, and Sergio Palazzo "Improving Energy Saving and Reliability in Wireless Sensor Networks Using a Simple CRT-Based Packet-Forwarding Solution, "IEEE/ACM Trans.. on networking , vol. 20.no1,Feb 2012.

[2] J.-H.Hong, C.-H.Wu, and C.-W.Wu, "RSA cryptosystem based on the Chinese Remainder Theorem," in Proc. ASP-DAC, Yokohama, Japan, Jan. 2001, pp. 391–395.

[3] G. Anastasi, M. Conti, M. Di Francesco, and A. Passarella, "How to prolong the lifetime of wireless sensor network," in Handbook of Mobile Ad Hoc and Pervasive Communications. Valencia, CA: American Scientific Publishers, 2007, ch. 6.

[4] E. Fasolo, M. Rossi, J. Widmer, and M. Zorzi, "In-network aggregation techniques for wireless sensor networks: A survey," IEEEWireless Commun., vol. 14, no. 2, pp. 70–87, Apr. 2007.

[5] S. Dulman, T. Nieberg, J. Wu, and P. Havinga, "Trade-off between traffic overhead and reliability in multipath routing for wireless sensor networks," in Proc. WCNC, New Orleans, LA, Mar. 2003, pp.1918-1922.

[6] B. Deb, S. Bhatnagar, and B. Nath, "ReInForM: Reliable information forwarding using multiple paths in sensor networks," in Proc. 28th Annu. IEEE LCN, Bonn, Germany, Oct. 2003, pp. 406–415.

[7] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly resilient, energy efficientmultipath routing in wireless sensor networks,"Mobile Comput. Commun. Rev., vol. 5, no. 4, pp. 10–24.

[8] P. Djukic and S. Valaee, "Minimum energy reliable ad hoc networks," in Proc. 22nd Bienni. Symp. Commun., Kingston, ON, Canada, Jun. 2004, pp. 150–152.

[9] [Online].Available:http://www.isi.edu/nsnam/ns/index.html