Volume 3, Issue VII, July 2015
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS…..

RELIABLE AND SECURE DATA TRANSMISSION IN WIRELESS SENSOR NETWORKS

Manisha[1], Mamta Sachdeva[2]

[1]M.Tech(CSE)
Computer Science and Engineering Department
South Point Institute of Technology & Management
DCRUST, Murthal India
manisha.antil275@gmail.com
[2]Associate Professor
Computer Science and Engineering Department
South Point Institute of Technology & Management
DCRUST, Murthal India

Abstract: *Wireless sensor networks can be utilized in a broad variety of applications ranging from battlefield surveillance in military, through remote patient monitoring in medicine to forest fire detection in environmental applications. Majority of WSN applications require at least some level of security. In order to achieve the needed level, secure and robust routing is necessary. Secure data transmission is a critical issue for wireless sensor networks (WSNs). Clustering is an effective and practical way to enhance the system performance of WSNs. Cluster-based data transmission in WSNs has been investigated by researchers to achieve the network scalability and management, which maximizes node lifetime and reduce bandwidth consumption by using local collaboration among sensor nodes. In this work, we have designed a routing protocol named reliable and secure data transmission protocol (RSDT) which is secure and reliable and the results will be compared with other routing protocols of same category such as secure and efficient data transmission (SET) protocols for WSNs, called SET-IBOOS, the identity-based online/offline digital signature (IBOOS) scheme. RSDT will use same concept of signature as used in SET-IBOOS.*

Keywords: *WSN, Secure WSN, Energy Efficient WSN, Hierarchical routing, cluster head*

1. INTRODUCTION

Wireless sensor networks consist of many small compact devices, equipped with sensors (e.g. acoustic, seismic or image sensors), that form a wireless network. Each sensor node in the network collects information from its surroundings, and sends it to a base station, either from sensor node to sensor node i.e. multi hop, or directly to a base station i.e. single hop [1].A wireless sensor network may consist of hundreds or up to thousands of sensor nodes and can be spread out as a mass or placed out one by one. The sensor nodes collaborate with each other over a wireless media to establish a sensing network, i.e. a wireless sensor network. Because of the potentially large scale of the wireless sensor networks, each individual sensor node must be small and of low cost. The availability of low cost sensor nodes has resulted in the development of many other potential application areas, e.g. to monitor large or hostile fields, forests, houses, lakes, oceans, and processes in industries. The sensor network can provide access to information by collecting, processing, analyzing and distributing data from the environment [2]. In many application areas the wireless sensor network must be able to operate for long periods of time, and the reliability as well as security of transmitting data is necessary [1].

2. RELATED WORK

In this paper [1], The authors propose two secure and efficient data transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the identity-based digital signature (IBS) scheme and the identity-based online/offline digital signature (IBOOS) scheme, respectively. In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing domain. SET-IBOOS further reduces the computational overhead for protocol security, which is crucial for WSNs, while its security relies on the hardness of the discrete logarithm problem. The authors show the feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks. In [2], the authors formulate the secret-sharing-based multipath routing problem as an optimization problem. The disjoint multipath routing scheme with secret sharing is widely recognized as one of the effective routing strategies to ensure the safety of information. This kind of scheme transforms each packet into several shares to enhance the security of transmission. A three-phase disjoint routing scheme called the Security and Energy-efficient Disjoint Route (SEDR) is proposed. Based on the secret-sharing algorithm, the SEDR scheme dispersively and randomly delivers shares all over the network in the first two phases and then transmits these shares to the sink node. The authors in [3] presented a new routing mechanism, which integrates FEC codes and selective encryption scheme for providing both QoS and secure data transmission in WSN. In the proposed protocol, RS coding is used to provide reliability and security. The sink node decides on the paths selection process in order to satisfy the reliability or the delay requirements by an application and the number of these paths is determined to enhance the reliability. The research article [4] presents the development of the real test bed of BIOSARP routing protocol. The test bed consists of 10 sensor nodes (TELOSB). The BIOSARP routing protocol based WSN performs well and its adaptable behavior to the environmental changes ensures reliable data transfer. In [5], the authors propose and evaluate the performance of a secure routing protocol that take into account the existence of multi path between sender and destination to transmit data in several paths. In [6], the authors present an algorithm to enable the base station to securely compute predicate count or sum even in the presence of such an attack. This attack-resilient computation algorithm computes the true aggregate by filtering out the contributions of compromised nodes in the aggregation hierarchy. The research community proposed a loss-resilient aggregation framework called synopsis diffusion, which uses duplicate insensitive algorithms on top of multipath routing schemes to accurately compute aggregates (e.g., predicate count or sum).In [7], the authors presented a WSN routing protocol defined as Biological inspired Self-Organized Secure Autonomous Routing Protocol (BIOSARP) enhances Secure Real-Time Load Distribution (SRTLD) with an autonomous routing mechanism. In the BIOSARP mechanism, an optimal forwarding decision is obtained by using improved Ant Colony Optimization (IACO). In IACO, the pheromone value/probability is computed based on the end-to-end delay, remaining battery power, and link quality metrics. The proposed BIOSARP has been designed to reduce the broadcast and packet overhead in order to minimize the delay, packet loss, and power consumption in WSN. In [8], the authors design an end to end secure communication protocol in randomly deployed WSNs. The protocol is based on a methodology called differentiated key pre-distribution. The core idea is to distribute different number of keys to different sensors to enhance the resilience of certain links. The authors also provide detailed discussion on a potential attack (i.e. biased node capturing attack) to our solutions, and propose several countermeasures to this attack. An energy-efficient secure routing protocol for WSNs with a stationary sink is proposed in [9]. Using the location information of the sink, the proposed routing protocol builds the sink-oriented grids to ensure the path availability from the source to the sink. Choosing the next hop dynamically by taking the advantage of the node location and residual energy information, an energy-efficient path for data delivery is selected. The authors [10] have designed new pair wise key establishment schemes in WSN using deterministic pre distribution techniques based on combinatorial designs. Combinatorial trades were applied for the first time for key pre distribution in WSNs. The authors also present a new construction of strong Steiner trades. The authors initiated the study of triple key distribution in sensor networks, and applied it in secure routing, secure data aggregation and in communication in clustered sensor networks. Polynomial-based scheme is applied so that every three nodes indeed have a common (and unique) key. This scheme is c-secure, where c is degree of polynomials used. The authors [11] present the Secure SOurce-BAsed Loose Synchronization (SOBAS) protocol to securely synchronize the events in the network, without the transmission of explicit synchronization control messages. In SOBAS, nodes use their local time values as a onetime dynamic key to encrypt each message. In this way, SOBAS provides an effective dynamic en-route filtering mechanism, where the malicious data is filtered from the network. In this work [12], the authors presented a distributed security framework (DSF) for heterogeneous wireless sensor networks. In this framework, the authors dynamically use the available memory space of regular nodes to store a subset of defense schemes to provide security against multiple attacks. The gateway is responsible for updating this subset according to the current likelihood of the occurrence of an attack in its cluster. Warning scheme can enable the regular nodes to install the defense schemes in advance of potential forthcoming attacks. In this paper [13], the authors propose a routing technique to provide adequate source-location privacy with low energy consumption. The authors introduce this technique as the Sink Toroidal Region (STaR) routing. With this technique, the source node randomly selects an intermediate node within a designed STaR area located around the SINK node. The STaR area is large enough to make it unpractical for an adversary to monitor the entire region. Furthermore, this routing protocol ensures that the intermediate node is neither too close, nor too far from the SINK node in relations to the entire network.

3. IBOOS SCHEME FOR CLUSTERED WIRELESS SENSOR NETWORK

An IBOOS scheme [1] implemented for CWSNs consists of following four operations, specifically, setup at the BS, key extraction and offline signing at the CHs, online signing at the data sending nodes, and verification at the receiving nodes [1]:

I. Setup. The BS (as a trust authority) generates a master key msk and public parameters param for the private key generator (PKG), and gives them to all sensor nodes.
II. Extraction. Given an ID string, a sensor node generates a private key sekID associated with the ID using msk.
III. Offline signing. Given public parameters and timestamp t, the CH sensor node generates an offline signature SIG offline, and transmits it to the leaf nodes in its cluster.
IV. Online signing. From the private key sekID, SIG offline and message M, a sending node (leaf node) generates an online signature SIG online.
V. Verification. Given ID, M, and SIG online, the receiving node (CH node) outputs “accept” if SIG online is valid, and outputs “reject” otherwise.

In Step 1, at the beginning of the setup phase of a new round, the BS first broadcasts its ID, a nonce (number used once), and the denotation of the starting time Ts of the current round to all sensor nodes, which is used for the signature signing and verification in the setup phase. In Step 2, a sensor node decides whether to become a CH for the current round, based on the threshold T(n) compared with numbers from 0 to 1, which is set as follows:

$$T(n) = \frac{\rho}{1-\rho\times\left(r \bmod \left\lfloor\frac{1}{\rho}\right\rfloor\right)}\cdot\frac{E_{cur}(n)}{E_{init}(n)} \qquad \forall n \in G_n,$$
$$T(n) = 0 \qquad \forall n \notin G_n. \tag{1}$$

Dynamic clustering algorithm preferably with multiplying the ratio of residual energy of the current sensor node (i.e., Ecur(n)/Einit(n)) to increase the energy efficiency in the clustering, where Ecur(n) is the current energy, and Einit(n) is the initial energy of the sensor node. ρ is a priori determined value which stands for the desired percentage of CHs during one round (e.g., ρ = 10%), r is the current round number, and Gn is the set of sensor nodes that have not been CHs in the last 1/ ρ rounds. If the value of determined number is less than the threshold, the sensor node elects itself as a CH. The sensor node who decides to become a CH broadcasts the advertisement message (adv) to the neighboring nodes in the network, which is concatenated with the signature.

In Step 3, the sensor node, which decides to be a leaf node, picks a CH to join based on the largest received signal strength of adv messages. Then, it communicates with CH I by sending a join_request (join) message, which is concatenated with the destination CH's ID IDi, its own ID IDj, time stamp Ts, and the digital signature.

In Step 4, a CH i broadcasts an allocation message to its cluster members for communication during the steady-state phase, yet to be concatenated with the signature.

In Step 5, according to the TDMA schedule from Step 4, each leaf sensor node j transmits the encrypted data Cj in a packet to its CH. In this way, each CH collects messages from all members in its cluster, aggregates and fuses data.

In Step 6, CHs send the aggregated data F to the BS, yet to be concatenated with the digital signature. The steady-state phase consists of multiple reporting cycles of data transmissions from leaf nodes to the CHs, and is exceedingly long compared to the setup phase.

In this way, energy consumption of each and every node is calculated. This process will be repeated until the whole network gets down or number of rounds finished.

4. METHODOLOGY

The foundation of proposed protocol lies in the realization that the base station is a high-energy node with a large amount of energy supply. Thus, proposed protocol utilizes the base station to control the coordinated sensing task performed by the sensor nodes. In proposed protocol, the following assumption are to be considered.

- A fixed base station is located in center of the region
- The sensor nodes are energy constrained with a uniform initial energy allocation.
- The nodes are equipped with power control capabilities to vary their transmitted power.
- Each node senses the environment at a fixed rate and always has data to send to the base station.
- All sensor nodes are immobile.
- The Key concept of SET-IBOOS is used as it ease. So, we assume that we are securing the data in same way as in IBOOS.

The radio channel is supposed to be symmetrical. Thus, the energy required to transmit a message from a source node to a destination node is the same as the energy required to transmit the same message from the destination node back to the source node for a given SNR (Signal to Noise Ratio). Moreover, it is assumed that the communication environment is contention and error free. Hence, there is no need for retransmission.

The steps of the algorithm are:

1. Initially, base station is set up at the center of region and nodes are setup in that particular region and each node will have equal energy.

2. In round 1, Cluster Head will be created according to probability condition.

3. The decision of each node to become cluster head is taken based on the suggested percentage of cluster head nodes *p*. A sensor node chooses a random number, *r*, between 0 and 1. If this random number is less than a threshold value, *T (n)*, the node becomes a cluster-head for the current round. The threshold value is calculated based on an equation that incorporates the desired percentage to become a cluster-head, the current round, and the set of nodes that have not been selected as a cluster-head in the last (1/*P*) rounds, denoted by G. *T (n)* is given in eq. (1).

Optimal number of cluster heads is estimated to be 10% of the total number of nodes.

Probability of node to become cluster head will vary according to given equation:

p (i)= P * n * RE *EN / (TE* Ea) (2)

where, P= probability to become cluster head which is 0.1.
n = no. of nodes
RE= remaining energy of a particular node
EN = Initial energy of a particular node
TE = Total Energy of the Network
Ea = Average energy of network

Average energy of network is given by equation:

Average energy= TE * (1-r / rmax) / n; (3)

where, TE = Total Energy of the Network
r = current round
rmax= total no. of rounds
n = no. of nodes

Now, the modified formula for choosing cluster head is given in eq (1).

4. Then, Nodes sends the data to their respective cluster heads and energy consumption will be calculated.

5. Cluster Head will aggregate the data and send it to the base station and energy consumption will be calculated for each node and cluster heads.

6. In round 2, the nodes will become cluster heads according to probability condition i.e. according to minimum distance from base station and threshold energy.
7. After selection of cluster heads, Nodes sends the data to their respective cluster heads, that will be selected according to the minimum distance of a particular node from cluster heads and energy consumption will be calculated.
8. Cluster Head will aggregate the data and send it to the base station and energy consumption will be calculated.
9. This process will be repeated until the whole network gets down or number of rounds finished.
10. Performance will be evaluated according to parameters like network lifetime, energy dissipation, no. of data packets sent etc.
11.

5. IMPLEMENTATION AND RESULTS

5.1 Parameter Value

Table 1. Network Parameters

Network field:	100 x100m
N (Number of nodes):	100
Initial energy:	1 J
Eelec (ETx&ERx):	50nJ/bit
ε fs (free space):	10 pJ/bit/m^2
εmp:	0.0013 pJ/bit/m^4
E_{DA}:	5 nJ/bit/signal
Eoff:	5 μJ/ signature
Eon:	12.37 μJ/ signature
Data packet size:	4000 bits
Tool used:	MATLAB 7.6.0

5.2 Results

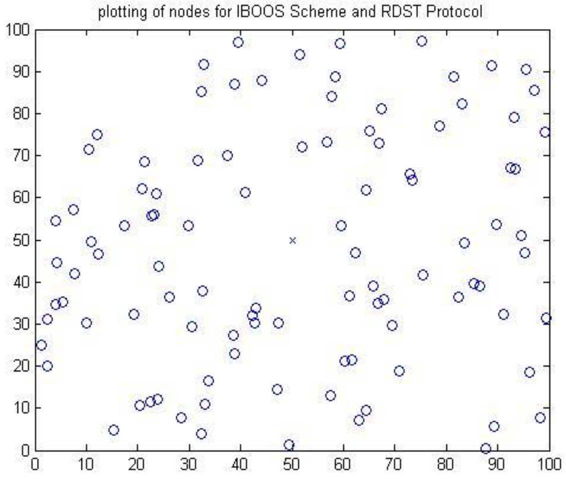

Figure 1: Deployment of nodes and base station

Figure 1 shows the deployment of nodes and base station in a particular region. The region we have taken for simulation is 100m x 100m. The 'o' symbol denotes the nodes and 'x' symbol denotes the base station (sink). The position of nodes is taken similar in both techniques IBOOS as well as in RSDT protocol.

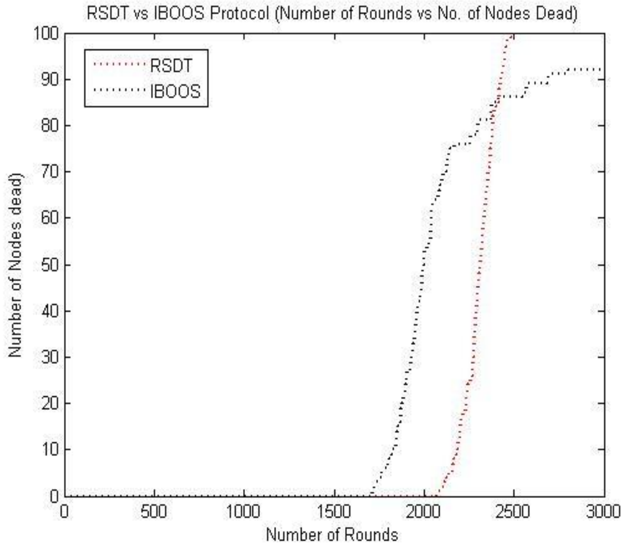

Figure 2: Number of Rounds vs Number of Nodes Dead

Figure 2 shows the comparison of routing protocols identity-based online/offline digital signature (IBOOS) scheme, and reliable and secure data transmission protocol (RSDT) in terms of Number of nodes dead. Figure 2 shows the overall lifetime of the network. Here, we can observe that RSDT performs better in comparison to IBOOS in sending data to base station. Around 80% of network performs better in comparison to IBOOS.

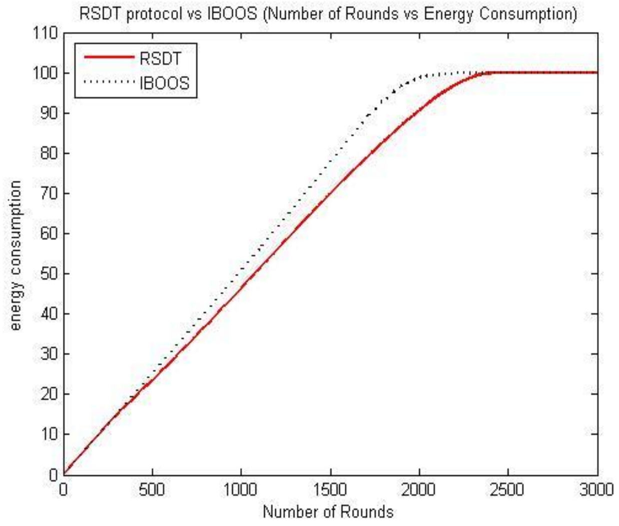

Figure 3: Number of Rounds vs Energy Consumption

Figure 3 shows the lifetime of the network. It shows that how energy of the network consumes step by step and finally whole network goes down. It can be observed from the figure 3 that, RSDT consumes less energy and sustain more number of rounds as compare to IBOOS protocol.

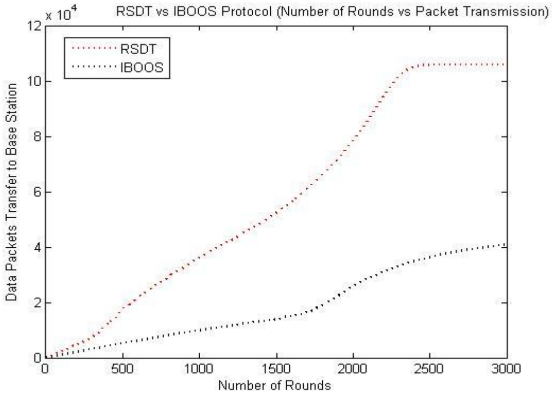

Figure 4: Number of Rounds vs Data Packets sent to base station

Figure 4 shows how much data will be sent from nodes to SINK. From figure 4, we can observed that, in IBOOS protocol data sent to base station is relatively less as compared to RSDT.

Table 2: Network Lifetime

When First Node dies		When 30% of Nodes dies		When 80% of Nodes dies	
IBOOS	RSDT	IBOOS	RSDT	IBOOS	RSDT
1713	2070	1930	2274	2299	2383

Table 2 shows the network lifetime comparison between IBOOS and RSDT protocol. IBOOS first node is died after 1713 rounds whereas RSDT first node died after 2070 rounds. More survival of rounds means network lifetime will increases, which finally increases the packet transfer to base station and hence RSDT will become more reliable as compare to IBOOS.

6. CONCLUSION AND FUTURE SCOPE

WSNs differ from traditional wireless communication networks in several of their characteristics like reliability of data, power awareness, security etc. This new routing protocol named Reliable and secure data transmission protocol (RSDT) which is hierarchical routing based with the whole control to the base station or we can say that base assisted. While self-configuring, the nodes are unaware about the whole logical structure of the network. But in Reliable and secure data transmission protocol (RSDT), the base station first collects information about the logical structure of the network and residual energy of each node. So, with the global information about the network base station does cluster formation better in the sense that it has information about the residual energy of each node. Finally, Reliable and secure data transmission protocol (RSDT) is compared with already developed routing protocol IBOOS. A comparison of these is done on the basis of energy dissipation with time, system lifetime of network and number of packets sent to base station.

In WSN, hundreds or thousands of sensor nodes are randomly scattered in the sensor field. These nodes sense the data and send this sensed data to the cluster head (in case of hierarchical routing) or directly to the base station according to the TDMA (time division multiplexing access) given by cluster head or base station respectively. In future, the work can be enhance to design a routing protocol which is more energy-efficient and secure for Wireless Sensor Networks by applying genetic algorithm or some other optimization technique to fix base station in an area where it can cover maximum nodes.

REFERENCES

[1] Huang Lu, “Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 3, MARCH 2014 pp. 750- 761.

[2] Anfeng Liu, Zhongming Zheng, “Secure and Energy-Efficient Disjoint Multipath Routing for WSNs”, *IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY*, VOL. 61, NO. 7, SEPTEMBER 2012.

[3] Hind Alwan, and Anjali Agarwal ,” A SECURE MECHANISM FOR QOS ROUTING IN WIRELESS SENSOR NETWORKS”, *IEEE*, 2012.

[4] Kashif Saleem , “A Real-Time Empirical Study of BIOSARP based Wireless Sensor Network Testbed”, *IEEE*, 2012.

[5] Lynda Mokdad, “Performance evaluation of security routing strategies to avoid DoS attacks in WSN”, *IEEE*, 2012.

[6] Sankardas Roy, “Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker’s Impact “, *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, VOL. 9, NO. 4, APRIL 2014.

[7] Kashif Saleem, “Empirical Studies of Bio-inspired Self-Organized Secure Autonomous Routing Protocol “,*IEEE*, 2013.

[8] Wenjun Gu, Neelanjana Dutta, Sriram Chellappan, and Xiaole Bai, “Providing End-to-End Secure Communications in Wireless Sensor Networks“, *IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT*, VOL. 8, NO. 3, SEPTEMBER 2011.

[9] Huei-Wen Ferng and Dian Rachmarini , “A Secure Routing Protocol for Wireless Sensor Networks with Consideration of Energy Efficiency”, *IEEE*, 2012.

[10] Sushmita Ruj, Amiya Nayak, “Pairwise and Triple Key Distribution in Wireless Sensor Networks with Applications”, *IEEE TRANSACTIONS ON COMPUTERS*, VOL. 62, NO. 11, NOVEMBER 2013.

[11] A. Selcuk Uluagac, “Secure SOurce-BAsed Loose Synchronization (SOBAS) for Wireless Sensor

Networks”, *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS*, VOL. 24, NO. 4, APRIL 2013.

[12] Himali Saxena, “DSF - A Distributed Security Framework for Heterogeneous Wireless Sensor Networks”, *IEEE*, 2010.

[13] Leron Lightfoot, “Preserving Source-Location Privacy in Wireless Sensor Network using STaR Routing”, *IEEE*, 2010.