



Enhanced Approach for Reliable & Secure Wireless Sensor Network

Ravi Kumar¹, Sunil Kumar², Prabhat Singh³

Computer Science Department

ABES Engineering College, Ghaziabad, India

Abstract: Modern wireless sensor networks require specific and high degree of security due to their limitation and versatility tasks. The absence of permanent infrastructure makes these networks suitable for many civilian applications. But their limited computational ability and battery resources restrictions makes them vulnerable to many kinds of attacks. This paper presents reliability in Wireless Sensor Network (WSN) information transmission, which can be used to exactly estimate the system working quality. The WSN reliability mathematical calculation approach gives insight on how to secure WSN through reliable backbone connectivity, reliable sensor network and data aggregation. Solutions to meet WSN security interconnectivity reliability, network reliability and data aggregation scheme for robust security systems designing have been introduced.

Keywords: Networks, Sensor Network Security, WSN, Design, Security, Data delivery, Reliability.

1. Introduction

Sensor networks are being deployed in situations where it is important to protect the message communication from eavesdropping or tampering. Wireless Sensor network (WSN) consists of sensor nodes which are deployed in versatile and often potentially hostile environment, responsible for sensing, processing, and transferring environmental information on the sensor field towards the sink node that is often referred to as BS (Base Station) as can be seen on figure one below. The absence of fixed infrastructure and cost effectiveness makes WSN ideal for civilian applications such as disaster relief, emergency rescue operations, patient monitoring, environmental control, military applications such as target identification and tracking as well as surveillance networks. These applications require that sensor networks offer a high degree of security. An adversary can thwart the work of any part of the network by perturbing the information produced, stopping production, or pilfering information to all what has been mentioned above as function or application of WSN. To reduce the vulnerability paper [1] argues that, the WSN design must balance traditional objectives such as energy efficiency, cost, and application level performance with security to the higher degree than attacker's competence. The authors in [2] developed architecture and associated algorithms to build a self-organizing WSN system that is capable of detecting mobile targets using cooperative sensors that are randomly deployed in a physical environment. The primary focus presented in manuscript [3] is to providing security mechanisms that enables the secure operation of in-network processing, a key emerging theme in the design and deployment of WSN. Jones et al. in [4] described a WSN model and proposed a solution which uses parameterized frequency hopping and cryptographic keys to provide differential security services and readily applicable to WSNs having anonymous nodes that are unaware of location. Perrig *et al* also proposed *SPINS* [5], a general security infrastructure for WSN. The infrastructure consists of an encryption primitive; *SNEP*, and an authenticated streaming broadcast primitive, *micro TESLA* have been well discussed in [14]. In [6], an algorithm to reliably transfer data by using one-phase pull directed diffusion, a data-centric routing technique in WSNs have been presented. However the research in papers [7, 14] presents the ideas on how to improve and enhance security and performance of an Ad Hoc networks through a multipath routing strategy and cipher block chaining. Consequently, that makes us to believe that existing security mechanisms are inadequate, and new ideas are needed. Fortunately, the new problems also inspire new research and represent an opportunity to properly address sensor network security from the start. Motivated with existing research gaps in WSN security we formulate our findings based on three main questions, where by first is what are the requirements for designing reliable security system? Second is how to estimate total WSN reliability which includes backbone interconnection and each WSN components and third is how to design mathematical model of reliable security system and calculate non-failure operation probability which we further examine in details from sections 3-4 below. We assume that the node failures are statistically independent and imagine that the node meantime- to-failure (*MTTF*) is relatively large compared to the message transmission time, the maximum propagation delay, and, the time required by the network to adapt to topology changes due to failures. Therefore the possible estimate of the operational probability is calculated as $MTTF / (MTTF + MTTR)$ as detailed in section four of the paper. The rest of the paper is organized as follow; Section 2 presents the requirements for WSN security and advantages of our approach. Proposed reliability approach and data aggregation for security is presented in

section 3. The paper evaluates security verification of WSN mathematically and system working reliability in sections 4 and gives conclusion in section 5

2. Security Requirements For Wsn

In many ways security has been viewed as a standalone component of a system's architecture or afterthought, where a separate module provides security. This separation is, however, usually a flawed approach to network security. To achieve a secure system, security must be integrated into every component. In many cases not integrating security to components during system development design, component has turned to be a point of attack. As a result, security must pervade every aspect of system design. The proposed approach addresses several aspects, being very flexible and able to be easily adapted to different kinds of scenarios when compared with the available approaches in [15, 17] To design reliable WSN security system, we follow the reliability approach taking advantage of security requirements in a following sequence:

1. Complex parameters for reliability (operational availability coefficient, availability, operating efficiency);
2. Reliability requirements (reliability probability, average time before denial of service, on denial and on fault);
3. Time requirements (various time resources and life time);
4. Reparability requirements (time for repairing average active state (serviceable condition), time allowable for repair);
- 5 Different types of dependability measures which can be obtained from the same model (e.g., reliability, availability, MTTF) as well as the criticality of the network devices (Birbaum's measure). The reflection of reliability requirements noticed above gives us the general idea of setting up the calculation of WSN reliability through interconnected backbone, WSN component (sensor nodes) which characterizes quality of the total working system and data aggregation which can support in providing accurate aggregation results securely without exhausting the network.

3. Complexity Of Wsn Reliability

We consider WSN as a complex system consists of three components: sensor nodes grouped to clusters, task manager node (user, base station) and interconnect backbone [8], as shown in Figure 1. below. Each Sensor Node contains various sensors and actuators that are used to collect let's say environmental data, process and transmit them. Collected data are transferred to the base station through the network.

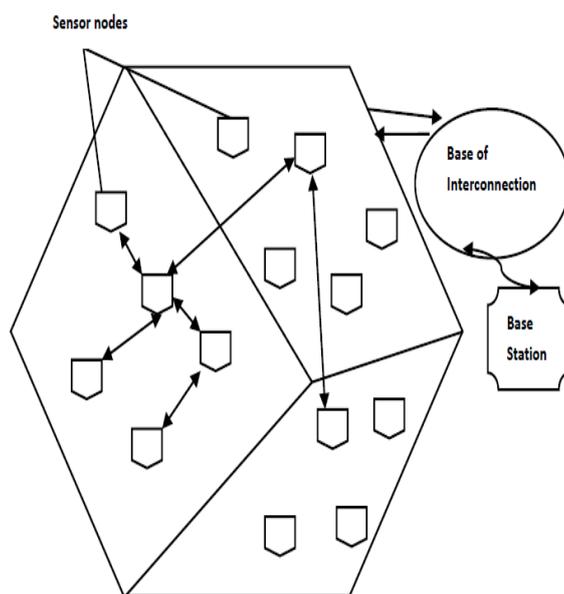


Fig 1. Configuration architecture of Wireless sensor network

Direct communication between individual nodes may be required sometimes. Base station performs tasks in data storage, analysis, and display and control interface backbone interconnectivity. Due to less stringent limitations, it can perform significantly more complex tasks than WSN nodes. Therefore to calculate complex WSN reliability it's important to compute the reliability of each WSN component (interconnected backbone and nodes organized to clusters [9, 10, 11]). We assume a sensor to be a device that possesses three basic capabilities: sensing, computing, and communicating. Sleeping sensor consumes essentially no energy [15]. In our scenario sensor network is connected to the outside world through a sink node while having a full range of computational and communication capabilities and a renewable power supply. From the presented scenario we introduce how we calculate interconnectivity reliability for transmission as follow in section 3.1 below.

3.1 Reliability of Interconnectivity Backbone

To evaluate the reliability and availability of Wireless Sensor Networks our approach depends on bandwidth frequency of communication channel, signal power and noise relation. Therefore maximum transmitting channel bandwidth (A_{max}) can be calculated as follow:

$$A_{max} = N \log_2 (1 + Ls / Ln) \quad (1)$$

Where N backbone interconnectivity frequency; Ls signal power, Ln – noise power, $(1 + Ls / Ln)$ is number of signal level which can be accepted by receiver. E.g., Ls / Ln is 3 this means that power signal is more than noise power for three times; therefore single signal can transmit 4 values, i.e. $\log_2 (1 + 3) = 2$ bytes of data.

We calculate minimum time cycle (T_{min}) for signals transmission with F as follows:

$$T_{min} = 1 / (2N) \quad (2)$$

Then number of unmistakably bites (A) transmitted in channel per sec can be computed as:

$$C = 2F [1 + p \log p + (1 - p) \log (1 - p)], \quad (3)$$

Where p is probability of data distortion due to obstacles. This equation allows exactly estimation of interconnectivity backbone reliability.

3.2 Wireless Sensor network Reliability

In this presentation, it is assumed that sensor data readings are sent towards a sink. Sensors are assumed to periodically send data. Thus, the amount of data readings generated per time interval in the sensor field is known. Additionally it is assumed that packet losses are independent of additional factors such as message size and traffic density. Increases in message size will increase the probability of bit errors within a message, but, note that in many forms of aggregation, packet size remains unchanged or does not change significantly. Therefore we define *reliability* of a WSN as the probability that a minimum aggregate rate of information (L info) that can be delivered to the sink node.

However we characterize quality of the total working system by efficiency (Z) which depends in some parameters including reliability calculation from [12] and estimate it as follows:

$$Z = f(L_1, L_2, \dots, L_n, S) \quad (4)$$

Where L_1, L_2, \dots, L_n performance quality of WSN components; S - total reliability.

If assuming that Z_0 is effectiveness with absolute reliable system functioning, then $Z = GeffZ_0$

Where Kef means degree of degradation due to unreliability of WSN components. Effectiveness saving coefficient (Gef) is taken as an initial factor when analyze system reliability:

$$Gef = W/W_0 \quad (5)$$

The effectiveness saving coefficient for WSN is defined by character of exploitation circle. Exploitation circle of WSN can be presented as sequence of several conditions i.e. by $Y(t)$ function. If $y(t) = 1$ – serviceable condition; 0 system denied or on repair. In this case, reliability estimation corresponds to some function, i.e. $y_i(t)$ function, where i means particular system's element. Because of active time state, serviceable condition and repair time which are taken as random values, and $y_i(t)$ as a realization of random function $y(t)$. So $y_i(t)$ can be considered as mathematical operational model of WSN and named as realization of operational process. Then estimation of i^{th} realization, i.e. functional $\phi(y_i(t))$, as a realization of random quantity $\phi(y(t))$. And quantitative index of reliability R can be considered as operational mathematical of random quantity $\phi(y(t))$ which can be calculated as:

$$R = N \phi(y(t)) \quad (6)$$

where $\phi(y(t))$ operational mathematical of random quantity and where N is the required minimum number of sensor nodes.

The WSN reliability and network parameters, especially network reliability and data acquisition rate. Can improve security from the point of system analysis to quality of services, maximum data transport quantity and quality over network nodes and backbone connectivity can be calculated to ensure the safety flow of the information through sensor nodes.

In order to solve reliability problem task, i.e. finding total WSN reliability, we prove and analyze mathematically our approach as:

$$Z = f(x_1, \dots, x_n; z_1, \dots, z_n) \quad (7)$$

$$p_k = \psi(x_1, \dots, x_m; z_1, \dots, z_n) = 0 \quad (8)$$

Where Z - criterion of efficiency; x_1, \dots, x_m – controlled variables; z_1, \dots, z_n uncontrolled variables or random influence; p_k - restriction function. Assuming that criterion of efficiency Z is already chosen and there are two types (Z) as follows: Threshold damage as a result of attack. Attack here is considered implemented if damage is not less than threshold. In this case, efficiency criterion is a task performance probability and result can have only two values: 1 – the attack task overcoming completed by the system; or 0 – for the opposite case. Secondly, result of countermeasures increases steadily depending on damage increasing. In this case the goal of attack is not achievement of defined result but implementation of maximum damaging and efficiency criterion will be calculated as mathematical expectation damage.

3.3 Classification of Data Aggregation Scheme.

Data aggregation helps to prevent data redundancy in the network. As WSN's have high node densities, a node might receive the same data from more than one neighbour [16]. The paper presents the data aggregation classification for WSN, based on *aggregation method of quasi-parallelism*.

Quasi-parallelism means parallelism of service events which appear in system at the same time due to the following advantages it has for the security:

- Ability to reduce the size of the data transmitted through the network.
- Dynamic response to attack activities by executing of a self-healing mechanism.

• Dynamic aggregator election/rotation mechanism to balance the workload at aggregators.

These properties can support in providing accurate aggregation results securely without exhausting the network. In case of close interconnections between system components (M_i), and input signals of one component are the output components of another components, its possible do approximation between these system components mathematically, which makes it possible to design imitate model by module principle. If modules have its own unified structure with input, output and can manage events then these modules can be considered as *aggregators (A)*. Some system parts, input-output and information transmitting channels can be aggregators as well. Thus, *aggregator* is a function description of certain object in that aspects which influence on efficiency estimation of given system. Every aggregator has only input or output messages. Aggregator behaviour design is successive transitions chain from one state to another. Therefore we consider WSN security design as aggregation method of quasi-parallelism. Figure 2 presents communications of control program (CP) with aggregators where every aggregator approximates corresponding functional action ($FX_{i,j}$). A functional action realizes independency from each other.

Aggregators: $K_1 \{FX_{11}, FX_{12}, FX_{13}, FX_{14}\}$
 $K_2 \{FX_{21}, FX_{22}, FX_{23}\}$
 $K_3 \{FX_{31}, FX_{32}, FX_{33}, FX_{34}\}$

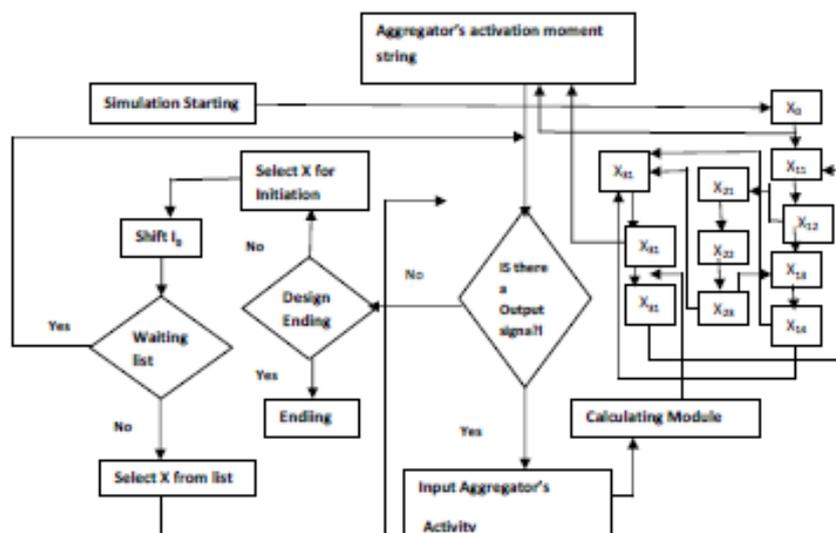


Fig.2 Simulation process (aggregator's activation process)

Every element has connection with another. We assume that there are only mono-channels for information transition in this scheme. A_0 is an influenced environment within-research system.

Example: Assume that z_{32} is output signal of aggregator X_{32} . Then time for next activation and output data list are set. Aggregator activation condition is set to serve the aggregator. Then the commutation matrix should be created for aggregators' communication. Having output signal z_{32} CP detects input signal by commutation matrix (x_{33}) and thus activates aggregator X_{33} . When all output signals Z_{ij} are served, the designed condition will finish its checks. The condition set will comprise

1. Choosing minimum time (t_{ij}) of aggregator states which can be used to select parameter location and aggregator's activation number at that moment.
2. This aggregator's number becomes initial value of aggregators' activation list and time model shift occurs: $t_{ij} = t_0 + \min t_{ij}$
3. The list of activated aggregators will form, i.e. aggregator activation moment which is equal to new model time t_0 which at the end of this process will initiate activation of successful aggregators.

Aggregator X_{ij} activation means to enable X_{ij} .

It is necessary to consider some conditions, for example initial setting of aggregates states at t_0 time, definition of next event time and corresponding aggregator, definition of new aggregator state and formation of input signals Y_{ij} as a result of changing inside states, checking of output signals and channel number by commutation matrix (S), defining new aggregate state by the input signal which are coming and form output signal. Therefore, is reasonable to use Aggregator method of imitate modeling with complex objects to secure WSN as with WSN it's feasible to take into consideration commutations matrix making. However signal serving will require additional machine time which is (key disadvantage) but aggregate approach will allow conveniently and strictly description of mathematical objects. Complex systems designing often use the following restriction; all component functional actions of real system are different. That's why the selection of quasi parallelism method was suitable to our approach. This method is especially effective for objects with high specialization of certain operations. In our case consisting of three components K_1, K_2, K_3 it' was convenient to consider each component as separate processes each of which describes one process class (setting process, program-process and input-output process) to ensure reliability of transmitted data.

4. Probability Verification Of Reliability Of The Proposed Wsn Approach

The guaranteed delivery of critical data is an essential requirement in most Wireless Sensor Network (WSN) applications. Illustrative examples are: battlefield surveillance, intrusion detection and E-health monitoring applications, where critical alerts must be timely and reliably delivered to the monitoring stations that act on those data; and industrial control applications, where commands must be timely and reliably delivered to the actuators (e.g., robotic arm). In this section we present mathematical reliability proof for WSN:

$$Z = P_{brk} P_{advr} X P(t), \quad (9)$$

where Z is efficiency criterion which to our case is dependence of efficiency on reliability, P_{brk} - is probability of system breaking without fault; P_{advr} - probability of security systems overcome by adversary; X - availability; $P(t)$ - probability of reliable operation within t -time.

From (9)

$$P_{info} = AP(t), \quad (10)$$

where P_{info} - probability of reliable operation. Subsequently

$$P_{info} = Z / P_{brk} P_{advr} \quad (11)$$

Using (11) we calculate P_{info} taking into consideration P_{brk} , P_{advr} and availability

$$X = MTBF / (MTBF + MTTR)$$

where MTBF and MTTR are mean time between failure and corresponding repair mean time, Mean Time between Failure (MTBF) Mean Time To Repair (MTTR). Then probability calculation of reliable operation depends on reliability of each WSN's component. We calculate it as follows:

$$P^*(t) = P_{rcl} P_{ich} P_{ibs}, \quad (12)$$

where $P^*(t)$ is probability of reliable operation based on reliability of each component, where P_{rcl} , P_{ich} , P_{ibs} are probabilities of reliable operation clusters, interconnect backbone and BS correspondingly [8, 13, 14]. Having these probabilities, we expect $P^*(t)$ to be established. Comparing $P^*(t)$ with required value, secured requirement measures can be assessed. Hence we can determine reliability in the following two ways:

1. Exploitation of nodes lifetime with minimum consumptions.
2. Maximum reliability requirements with given exploitation cost.

Solving the mentioned problems above "reliability-cost" direct searching approach can be used. Searching can be implemented by dynamic programming principle with maximization of objective function. This also is supposed to be an opening for future research and part of continuation of our work.

5. Conclusion

In Sensor Network environment security service are of utmost concern to end user. Reliability to wireless sensor network for security are studied in this paper. Our work reveals that reliability is dependent on three elements: connectivity, network parameters and Data aggregation. Data aggregation can influence the information transmitted within WSN in positive manner as illustrated in a proposed scheme and these influences can be used to control end-to end reliability of information delivery. An intuitive understanding of these relations and all the reliability criteria in this paper can be feasible for a general network parameter and security design.

References

- [1] Majeed A, Razak S., Ghazaleh A.B, A. Harras K.A 2009: TCP over Multi-Hop Wireless Networks: The Impact of MAC Level Interactions. ADHOC-NOW 2009: 1-15N.
- [2] Boudriga N., Baghdadi M., Obaidat M.S, 2006 "A New Scheme for Mobility, Sensing, and Security Management in Wireless Ad Hoc Sensor Networks," anss, pp.61-67, 39th Annual Simulation Symposium (ANSS'06).
- [3] Perrig, A. Szewczyk .R, Wen V., Culler D. and Tygar J.D, 2001 .SPINS: Security protocols for sensor networks, Proc. MOBICOM'2001, Rome, Italy.
- [4] Choi J., Choi B.Y, Song S., Hui Lee K.H, 2010: NQAR: Network Quality Aware Routing in Error-Prone Wireless Sensor Networks. EURASIP J. Wireless Comm. and Networking 2010
- [5] Koul A., R.B. Patel R.B, Bhat V.K, 2009"Double Split Based Secure Multipath Routing in Adhoc Networks," artcom, pp.835-839, 2009 International Conference on Advances in Recent Technologies in Communication and Computing.
- [6] Zia T. and Zomaya A.; 2006. Security Framework for Wireless Sensor Networks SAS – IEEE Sensors Applications Symposium, Houston, Texas USA, 7-9 FebrA,
- [7] Younis O. and Fahmy S. 2003,. MOBICOM, Distributed Clustering for Scalable, Long-; Lived Sensor Networks,
- [8] Ibriq J. and Mahgoub I, 2004. Cluster-based routing in wireless sensor networks: Issues and Challenges, SPECTS '04
- [9] Taherkordi A., Alkaee M. T and Sharifi M. 2006.Achieving Availability and Reliability in Wireless Sensor Networks Applications, Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06)
- [10] Chiasserini C.F. and M. Garetto . 2004. Modeling the Performance of Wireless Sensor Networks, IEEE INFOCOM.
- [11] Frolik J, 2004 .QoS Control for Random Access Wireless Sensor Networks, WCNC / IEEE Communications Society

- [12] Oreku G. S., Jiangzhong Li and Pazynyuk T., 2007. "An application-driven perspective on wireless devices security: the case of distributed denial-of-service (ddos)", Proceedings of the 2nd ACM workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks, Pages: 81 - 83, Chania, Crete Island, Greece.
- [13] Jang K.W, Lee S.H, Jun M.S, 2006 "Design of Secure Dynamic Clustering Algorithm using SNEP and TESLA in Sensor network," *ichit*, vol. 2, pp.97-102, 2006 International Conference on Hybrid Information Technology – Vol 2 (ICHIT'06)
- [14] Kumar G. , R. Mritunjay and L. Gang-soo ; 2012 Implementation of Cipher Block Chaining in Wireless Sensor Networks for Security Enhancement *International Journal of Security and Its Applications* Vol. 6, No. 1, January, 2012
- [15] AboElFotouh H., Shazly M., Elmallah E., Harms J. On area coverage reliability of wireless sensor networks. Proceedings of the 36th Annual IEEE Conference on Local Computer Networks (LCN '11); Bonn, Germany. 4–7 October 2011; pp. 584–592.
- [16] Valada A., David K., Kantor G.; 2010 "Design and Development of a Wireless Sensor Network System for Precision Agriculture" CMU-RI-TR-10-21.
- [17] Egeland G., Engelstad P. The availability and reliability of wireless multi-hop networks with stochastic link failures. *IEEE J. Sel. Areas Commun.* 2009;27:1132–1146.