SECURE TRANSMISSION OVER WSN VIA DECISION FUSION AND DISTRIBUTED DETECTION

V.PADMAPRIYA[*1]
M.Tech Student
Department of Communication Systems
PRIST University Pondicherry, India.

V.SARANYA[*2]
Assistant professor
Department of Communication Systems
PRIST University Pondicherry, India

ABSTRACT

In wireless device networks (WSNs), security and energy consumption are thought-about as durable technical challenges as sensors typically suffer from quality and energy constraints. During this paper, we have a tendency to study an easy and economical physical-layer security to supply knowledge confidentiality in a very distributed detection state of affairs. Specially, to forestall passive eavesdropping on transmission knowledge from sensors to AN ally fusion center (AFC), we have a tendency to propose a unique secret writing theme and call fusion rules for a parallel access channel model. The projected theme takes advantage of a free resource, i.e., randomness of wireless channels, to cipher the binary native call of every device in such how that the binary native call is flipped consistent with fast channel gain between the device and AFC. The location-specific and reciprocal properties of wireless channels alter the device and AFC to share the inherent randomness of wireless channels that don't seem to be on the market to an hearer. What is more, it's shown that the theme is well-suited to an occasional quality and energy economical modulation technique, no coherent binary frequency shift keying. to gauge performances of the projected theme, log-likelihood-ratio-based call fusion ways at the AFC area unit analyzed, and comparisons of call performances area unit disbursed. Additionally, we have a tendency to prove that the projected theme achieves excellent secrecy with an easy structure that's fitted to sensors of restricted quality.

KEYWORDS: *call fusion, distributed detection, eavesdropping, encryption, excellent secrecy, wireless device networks.*

I. INTRODUCTION

To resolve the technical challenge of secure communications in WSNs, there have been several notable approaches, where the ability of the physical layer is explored as a solution to the data confidentiality for the distributed detection in WSNs. Assuming the presence of a passive eavesdropper called an enemy fusion center (EFC), sensors in a WSN individually or collaboratively transmit their local decisions on a target state to an ally fusion center (AFC), where final decision is made. In this case, the central issue is how to design a physical layer scheme at the sensors to achieve reliable transmission with the AFC while preventing information leakage to the EFC. It is found that simultaneous transmission of local decisions using the type-based multiple accesses (TBMA) protocol over a multiple access channel (MAC) can be utilized for the data confidentiality in such a way that some sensors are deliberately selected to transmit interfering signals to make the EFC confused. Since all the transmitting data from sensors are naturally fused during transmission over MAC, the EFC is unable to remove the interfering signals, which thus hinders it from making a correct decision. In particular, the rule selecting the sensors generating interference is designed 1) to minimize the degradation of detection performance at the AFC and 2) to be autonomous and nondeterministic, which prevents the EFC from identifying the sensors generating interference

II. PROPOSED SYSTEM

To resolve the technical challenge of secure communications in WSNs, there have been several notable

ISSN: 2278 – 909X

approaches, where the ability of the physical layer is explored as a solution to the data confidentiality for the distributed detection in WSNs simultaneous transmission of local decisions using the type-based multiple access (TBMA) protocol over a multiple access channel (MAC) can be utilized for the data confidentiality in such a way that some sensors are deliberately selected to transmit interfering signals to make the EFC confused Achieving the information-theoretic perfect secrecy, which is not possible with traditional cryptographic techniques It is assumed that the AFC broadcasts a pilot signal to initiate distributed detection, and each sensor measures the strength of the received pilot signal, which is equivalent to measuring the magnitude of the channel gain (MCG) from the AFC to the sensor. Since a simple energy detector is enough to measure the pilot signal strength, the required additional complexity may be acceptable in many cases. Then, each sensor autonomously joins one of three groups dormant flipping non flipping groups, according to their MCG measurements whenever the AFC broadcasts the pilot signal. In the flipping and non flipping groups are called activated sensors they report their local decisions over a PAC in the time-division duplexing (TDD) manner. That is, the transmission from the sensors is carried out in the same coherence time over the same wireless channel where the pilot signal is broadcasted.

A. ADVANTAGES OF PROPOSED SYSTEM

- Energy consumption
- Secrecy of data transmission
- Randomness of wireless channel

B. PILOT SIGNAL

When we modulate and send a pilot carrier it become possible to detect the signal by envelope detection method which requires very less circuitry and is very cheap. Provided the sum of maximum amplitude of carrier and the message signal must be greater than zero so that the envelope gets a lift up.

C. ENERGY CONSUMPTION

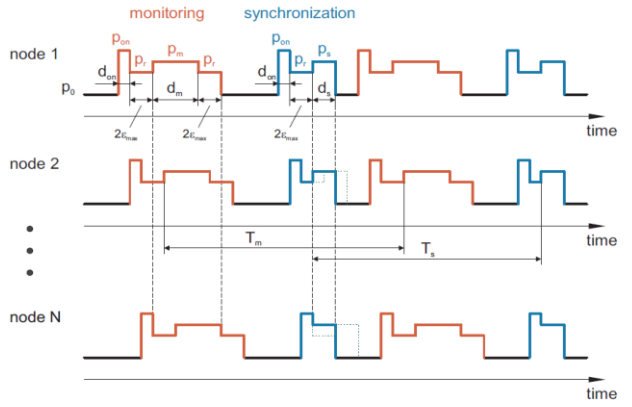

Fig. 1. Qualitative power consumption patterns during the execution of monitoring and synchronization tasks on various nodes of a WSN.

Fig 3.1 Energy Consumption of Various Nodes of WSN

D. ENERGY SAVING METHODS IN WIRELESS SENSOR NETWORKS

The work aims to identifying and quantifying energy saving methods in WSN. An important prerequisite to carry out this activity is to develop a methodology for the estimation of energy consumption in the individual WSN nodes and in the network as a whole. In the optimization for minimal energy consumption care should be taken to see that other parameters such as successful transmission of parameters by the network and event detection by the nodes are not sacrificed.

It is probable that only a combination of methods that attempt to reduce energy consumption at the node level and the network level will lead to a practical network that is energy efficient. Some of the methods that were thought of as promising are:

- Allowing nodes in a network to sleep for much longer periods during non -Transmission of data
- Minimize the time it takes for nodes to get into sleep mode and to awake from sleep Mode

E. PERFECT SECRECY

Perfect secrecy against eavesdropping, we further analyze the strength of our proposed scheme against two well known tacks in cryptanalysis where the EFC can

ISSN: 2278 – 909X

attempt to decrypt the captured signals without prior access to an encryption seed

***1) Known Plaintext Attack In cryptanalysis*:** It is assumed that an attacker can take some pairs of the plaintext and its encrypted data i.e., cipher text. In this case, the attacker can obtain secret information such as an encryption seed by analyzing correlation between them. This problem can happen in our scenario if the EFC has prior knowledge about the target state. Comparing the capture d signals (cipher text) from the activated sensors with the known target state (plaintext), the EFC can immediately know the group assignment of sensors and their individual encryption seeds. However, such an attempt to attack becomes in vain in our scheme, because each sensor update its encryption seed in every reporting session based on its instantaneous MCG, which is purely random and independent in each session. Even if the EFC obtains all the encryption seeds for activated sensors in a certain time period, they are disposable ones that are useless in the next reporting.

2) Brute Force Attack: Assuming that sensors are activated in a certain reporting session, there are no more than group assignments in our scheme. In this case, the EFC can try a brute force attack that checks all possible group assignments and figures out which one is highly likely. Then the Eve can deduce the target state. However, it can be easily showed that the two probabilities for the sensor to be involved in flipping and non flipping groups are the same under the condition of ,and group assignments are equally likely This is attributed by the following facts: a) the captured signals at the EFC are delivered through the eavesdropping channel that is independent of the main channel, and b) the activation probabilities are decided to be equal. Therefore, even though the EFC can consider all the possible group assignments for a small, the Eavesdropping is unable to recognize which sensors are in the flipping or none flipping groups

III. METHODOLOGIES

A. Encryption is performed as follows

We assume that a set of thresholds, where is predetermined and stored in every sensor The i–th sensor acquires its MCG, when the pilot signal is transmitted by the AFC and compares it with the thresholds in order to encrypt its local decision. If the ith sensor has the MCG satisfying, it is chosen to be in the none flipping

B. Algorithm for Perfect Secrecy

The main and eavesdropping channels are statistically independent when the EFC is located more than a half wavelength apart from both the sensors and AFC. It is done by log likelihood function; the total probability theorem is given by,

$$\begin{aligned} f\left(\mathbf{z}_i^E|\theta_\ell\right) &= \sum_{u_i}\sum_{\mathbf{x}_i} f\left(\mathbf{z}_i^E, \mathbf{x}_i, u_i|\theta_\ell\right) \\ &= \sum_{u_i} p\left(u_i|\theta_\ell\right) \sum_{\mathbf{x}_i} \int f\left(\mathbf{z}_i^E, h_i^S, \mathbf{x}_i|u_i, \theta_\ell\right) dh_i^S \\ &= \sum p\left(u_i|\theta_\ell\right) \sum \int f\left(\mathbf{z}_i^E|h_i^S, \mathbf{x}_i, u_i, \theta_\ell\right) \end{aligned}$$

Although the EFC is not aware of the MCGs of the main channels, we could assume that the encryption scheme performed in the sensors. By combining the above equation we can get,

$$\begin{aligned} &(1-P_{fi})\left(f\left(\mathbf{z}_i^E|\mathbf{E}(0)\right)\lambda_1 + f\left(\mathbf{z}_i^E|\bar{\mathbf{E}}(0)\right)\lambda_2\right) \\ &\quad + P_{fi}\left(f\left(\mathbf{z}_i^E|\mathbf{E}(1)\right)\lambda_1 + f\left(\mathbf{z}_i^E|\bar{\mathbf{E}}(1)\right)\lambda_2\right) \end{aligned}$$

C. TBMA Technique

The type-based multiple accesses (TBMA) approach can be exploited.

The following conditions for TBMA is following basic steps:

- Build up a time-limited waveform with finite energy.
- Let the aforementioned waveform go through an ideal low-pass filter the input outside the available bandwidth, and the output of the receiver filter within the original observation interval.

ISSN: 2278 – 909X

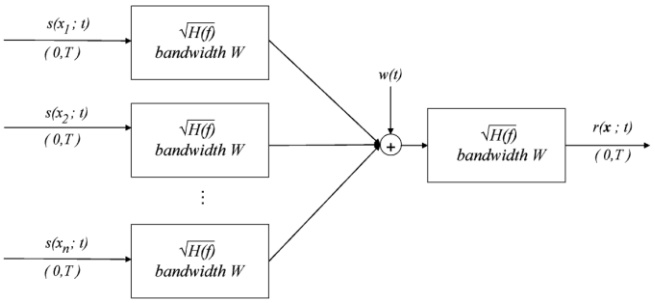

Fig 5.3 block scheme of the TBMA technique model

The transmission scheme whose idealization is represented by the signal in (6) would be actually feasible for our estimation purpose provided that the following is true:

- The noise component can be neglected for large, due to the increasingly large number of waveforms which are inherently added.
- The relevant (random) waveform is (on average) time limited and band limited.

D. Distributed Option

- For the distributed option we consider the local decision rule at the sensor nodes and the final decision rule at the control center, respectively. Local Decision Rule: As we have specified before, each sensor node applies a local decision rule to make a binary decision based on the T observations.
- A question yields naturally whether we should have an identical local decision rule for all the sensor nodes.
- Generally, an identical local decision rule does not result in an optimum system from a global point of view. However, it is still a suboptimal scheme if not the optimal one, which has been observed by some previous work.
- the binary hypothesis detection, no optimality is lost with identical local detectors in a two-sensor system
- Identical local detectors are asymptotically optimum when the number of sensors tends to infinity.
- We assume that each sensor node does not have any information about other nodes, which means that the identical local decision rule would depend only on {T, p, p0, p1}, while the number of sensor nodes K is considered as global information and not available for decision making of sensor nodes.
- Eventually the problem is simplified to a similar case for the centralized option, where the only difference is the number of observations changes from KT to T.

IV. MODULE DESCRIPTION

A. NODE COMPROMISE DETECTION

It is a critical security requirement for the successful deployment of large-scale wireless sensor networks. A node compromise attack often consists of three stages:

- The first stage is physically obtaining and compromising the sensors.
- The second stage is redeploying the compromised nodes back to the sensor network.
- The last stage is compromised sensors rejoining the network and launching attacks.

These two attacks are similar in the sense that they both generate black holes and the areas within which the opponent can either passively intercept or actively block information delivery. The objective of our study is to propose a randomized multi-path routing algorithm that can overcome the black holes formed by Compromised-node and denial-of-service attacks. Instead of selecting paths from a pre-computed set of routes, our aim is to compute multiple paths in a randomized way each time an information packet needs to be sent, such that the set of routes taken by various shares of different packets keep changing over time. As a result, a large number of routes can be potentially generated for each source and destination.

ISSN: 2278 – 909X

To intercept different packets, the adversary has to compromise or jam all possible routes from the source to the destination, which is practically infeasible. Depending on the type of information available to a sensor, we have develop our distributed scheme for propagating information shares called Purely Random Propagation (PRP). PRP utilizes only one-hop neighborhood information and provides baseline performance. To diversify routes, an ideal random propagation algorithm would propagate shares as depressively as possible.

B. RANDOMNESS OF WSN OVER MULTIPATH NODES

Consider a three-phase approach for secure information delivery in a WSN

- Secret sharing of information,
- Randomized propagation of each information share, and
- Normal routing (e.g., min-hop routing) toward the sink.

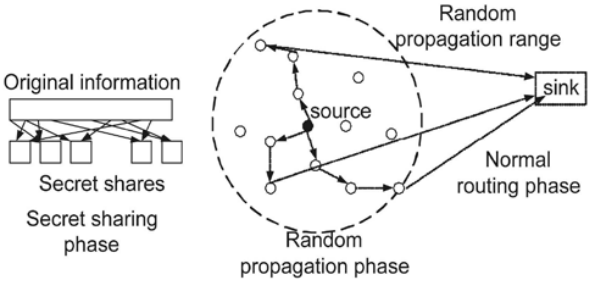

Fig 7.2 Routing in WSN's

More specifically, when a sensor node wants to send a packet to the sink, it first breaks the packet into M shares, according to a (T, M) –threshold secret sharing algorithm. Each share is then transmitted to some randomly selected neighbor. That neighbor will continue to relay the share it has received to other randomly selected neighbors, and so on.

In each share, there is a TTL field, whose initial value is set by the source node to control the total number of random relays. After each relay, the TTL field is reduced by 1. When the TTL value reaches 0, the last node to receive this share begins to route it toward the sink using min-hop routing. Once the sink collects at least T shares, it can reconstruct the original packet.

C. PURE RANDOM PROPAGATION (PRP)

Shares are propagated based on one-hop neighborhood information. More specifically, a sensor node maintains a neighbor list, which contains the of all nodes within its transmission range. When a source node wants to send data to destination, it includes a TTL of initial value N in each share. It then randomly selects a neighbor for each share, and uni-casts the share to that neighbor. After receiving the share, the neighbor first decrements the TTL. If the new TTL is greater than 0, the neighbor randomly picks a node from its neighbor list (this node cannot be the source node) and relays the share to it, and so on. When the TTL reaches 0, the final node receiving this share stops the random propagation of this share, and starts routing it toward the sink using normal min-hop routing.

D. SECURED DELIVERY OF PACKETS

In this module we can maintain the routing table; here we add one more column to maintain the packet delivery ratio. In this way we can maintain how many packets are transmitted over each path. It will be useful to identify any path and can packets handle packets number. We can stop transmission for some amount of time period over that path, so that the hacker cannot identify in which path the message is transmitted and also we can easily transmit the data securely.

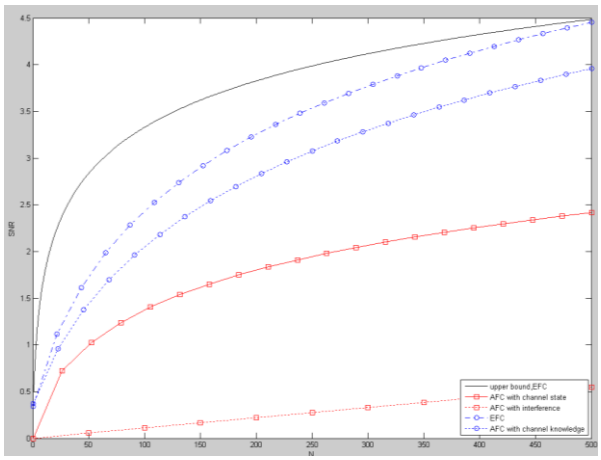

Fig 10.3 decode and forward relay with line space of nodes

ISSN: 2278 – 909X

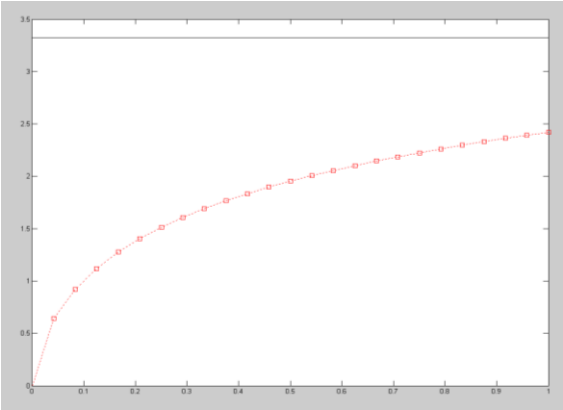

Fig 10.4 various link of SNR nodes

Channel statistics outperforms the conventional ones, and small performance loss is observed due to the high SNR approximation. Fair comparisons are cared by selecting sensors from the one with the highest MCG for the conventional scheme the number of sensors increases, the conventional scheme with a relative weak security level, i.e., ,loses its performance.

V. CONCLUSION

For a WSN where sensors report their binary local decisions over a PAC carefully utilizing a free natural resource, i.e., randomness of wireless channels, it is possible to make the EFC totally ignorant of the target state, i.e., perfect secrecy. The claim was thoroughly proved by information-theoretic point of view and also confirmed by performing numerical evaluations. The fusion rules with channel statistics and the high SNR approximation at the AFC for which performances are evaluated in terms of WEP at various SNR values and sizes of WSN. The evaluation verified that the proposed scheme results in a WEP of 0.5 at the EFC for perfect secrecy. In addition to the confidentiality, the reliability, i.e., WEPs at the AFC.Achieve perfect secrecy while maintaining superior WEP performances across wide ranges of SNR values and sizes of WSN.

REFERENCE

1) X.Chen, K.Makki, K.Yen, and N. Pissinou, "Sensor network security: A survey,"Commun.Surveys Tuts., vol. 11, no. 2, pp. 52–73, Second Quarter, 2009.

2) H.Jeon, D.Hwang, J. Choi, H. Lee, and J. Ha, "Secure type-based multiple access," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp.763–774, Sep. 2011.

3) T.C.Aysal and K. E. Barner, "Sensor data cryptography in wireless sensor networks," IEEE Trans. Inf. Forensics Security, vol. 3, no. 2,pp. 273–289, Jun. 2008.

4) V.Nadendla,"Secure Distributed Detection in Wireless Sensor Networks via Encryption of Sensor Decision,"M.S. thesis, Louisiana State University and Agricultural and Mechanical College, Baton Rouge,LA, USA, 2009.

5) S.Marano, V.Matta, and P.K.Willett, "Distributed detection with censoring sensors under physical layer secrecy," IEEE Trans. Signal Process. vol. 57, no. 5, pp. 1976–1986, May 2009.

6) C.Shannon, "Communication theory of secrecy systems," Bell Syst.Tech. J., vol. 28, no. 4, pp. 656–715, 1949.

7) J.Polastre, R.Szewczyk, C.Sharp, and D.Culler, The Mote Revolution: Low Power Wireless Sensor Network Devices Sep. 2004 [Online]. Available: http://webs.cs.berkeley.edu/papers

AUTHOR PROFILE

Ms.V.PADMAPRIYA, Presently Pursuing Final Year M.TECH Department of Communication Systems, In PRIST University, Puducherry Campus, Puducherry, India

Ms.V.SARANYA Received the M.Tech In. Presently she is a Working Assistant Professor in Communication Systems at PRIST University, Puducherry Campus, Puducherry, India.

ISSN: 2278 – 909X