ISSN: 2348-2079

MAY-2015

International Journal of Intellectual Advancements and Research in Engineering Computations

OPTIMAL BINARY DATA FUSION FOR DISTRIBUTED DETECTION IN WIRELESS SENSOR NETWORKS

[1]F. Jessy Nirmala, [2]K. P. Porkodi.

ABSTRACT

Wireless sensor networks (WSNs) are vulnerable to several types of attacks including passive eavesdropping, jamming, compromising (capturing and reprogramming) of the sensor nodes and insertion of malicious nodes into the network. Widespread adoption of WSNs, particularity for mission-critical tasks, hinges on the development of strong protection mechanisms against such attacks. Due to the scarcity of resources, traditional wireless network security solutions are not viable for WSNs. The life span of a sensor node is usually determined by its energy supply which is mostly expended for data processing and communication. Therefore, security solutions which demand excessive processing, storage or communication overhead are not practical. In particular, due to their high computational complexity, public key ciphers are not suitable for WSNs. An important application of WSNs, involves decentralized detection whereby the sensors send their measurements to an ally fusion center (AFC) which attempts to detect the state of nature using the data received from all the sensors .Due to the broadcast nature of the wireless media, the sensors data are prone to interception by unauthorized parties .

Considering the problem of secure detection in wireless sensor networks operating over insecure links. It is assumed that an eavesdropping fusion center (EFC) attempts to intercept the transmissions of the sensors and to detect the state of nature. The sensor nodes quantize their observations using a multilevel quantizer. Before transmission to the ally fusion center (AFC), the sensor nodes encrypt their data using a probabilistic encryption scheme, which randomly maps the sensor's data to another quantizer output level using a stochastic cipher matrix. The communication between the sensors and each fusion center is assumed to be over a parallel access channel with identical and independent branches and with each branch being a discrete memory less channel. Employ J-divergence as the performance criterion for both the AFC and EFC. The optimal solution for the cipher matrices is obtained in order to maximize J-divergence for AFC, whereas ensuring that it is zero for the EFC. With the proposed method, as long as the EFC is not aware of the specific cipher matrix employed by each sensor, its detection performance will be very poor. The cost of this method is a small degradation in the detection performance of the AFC. The proposed scheme has no communication overhead and minimal processing requirements making it suitable for sensors with limited resources. Numerical results showing the detection performance of the AFC and EFC verify the efficacy of the proposed method.

INTRODUCTION

Wireless Sensor Network(WSN) of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring and so on.

Wireless Sensor Networks (WSNs) are often deployed in hostile environments where an adversary can physically capture some of the nodes, first can reprogram and then, can replicate them in a large number of clones, easily taking control over the network.

Author for Correspondence:

[1]Final year ME, Al-Ameen Engineering College, Erode, Tamilnadu, India.

[2]Assistant Professor / CSE, Al-Ameen Engineering College, Erode, Tamilnadu, India.

RELATED WORK

Security of wireless sensor networks has been the subject of many studies in recent years for different attack strategies of the adversaries. In particular, countermeasures against passive eavesdropping have been proposed by a number of researchers. In [3] and [4], the authors propose an encryption scheme whereby a sensor may flip its local decision based on the instantaneous channel fading gain between itself and the AFC. The channel fading gains, which depend on the location of the sensors and AFC, are known to the AFC but are unknown to the EFC. They showed that information-theoretic perfect secrecy can be achieved. In [5], channel fading gains are used in a secure type based multiple access scheme where the sensors follow different reporting rules depending on the strength of their channel gains.

Probabilistic ciphers were also studied in [6] where a single cipher matrix is designed to minimize the error probability of AFC with a lower bound on the error probability of EFC. It was shown that it is possible to degrade the error probability of EFC significantly and yet, achieve very low error probabilities for AFC. The design approach is ad hoc and results in a suboptimal solution for the cipher matrix. In this paper we obtain the optimal solution for a set of cipher matrices. The numerical results in our proposed method here outperforms the method.

The authors have developed a security scheme where the sensors perform censoring in order to save energy. The relation between J-divergence and detection performance is elucidated by Stein's lemma. Censoring allows a sensor not to send its data when it does not provide a good indication of the state of nature. In this approach the sensor nodes transmit their observed likelihoods to the FC. The eavesdropper does not have access to the sensors' transmitted data but can monitor the transmission activity of the channel and exploit the busy/idle state of the channel for detecting the hypothesis. Kulbeck Leibler divergence is used as the cost function for both AFC and EFC and a censoring strategy is developed in order to maximize the divergence of AFC while ensuring that the divergence of EFC is zero. Our approach is different from several regards. The nodes here transmit their quantized observation and EFC is able to intercept the actual transmitted messages. While we also use divergence as the performance measure for AFC and EFC, security is provided through probabilistic ciphers.

Security in distributed detection has also been investigated by many authors in the context of Byzantine attacks. Here an adversary inserts a number of malicious nodes into the network which deteriorate the detection performance by transmitting false data. It is assumed that through collaboration, the Byzantine nodes are aware of the true hypothesis. The authors formulate the problem in the context of Kullback- Leibler divergence and obtain optimal attacking distribution for the Byzantine nodes using a water-filling procedure. In [11] the authors consider data fusion schemes in a network under Byzantine attack and propose techniques for identifying the malicious users. In [10] the authors consider adding stochastic resonance noise at the honest and/or Byzantines in order to enhance the detection performance. An algorithm based on expectation maximization is developed in [2] for decentralized detection in the presence of misbehaving nodes. Collaborative spectrum sensing in cognitive radio networks is identical to the classical decentralized detection and recently several papers have considered cooperative spectrum sensing in the presence of Byzantine attacks [9], [7], [8]. In particular several variations of the so called reputation-based algorithm have been proposed for data fusion and for the identification of the malicious nodes.

SECURITY GOALS FOR SENSOR NETWORKS

Sensor network security requirements are categorized into two types primary security requirements and secondary security requirements. The primary security requirements are Data Confidentiality, Data Authentication, Data Integrity and Data Availability. Data Freshness, Self-Organization, Time Synchronization and Secure Localization, are the secondary security requirements.

PRIMARY GOALS

Confidentiality is the ability to conceal messages from a passive attacker so that any message communicated via the sensor network remains confidential. This is the most important issue in network security. A sensor node should not reveal its data to the neighbors. Authentication ensures the reliability of the message by identifying

its origin. Attacks in sensor networks do not just involve the alteration of packets; adversaries can also inject additional false packets. Data authentication verifies the identity of the senders and receivers. Data authentication is achieved through symmetric or asymmetric mechanisms where sending and receiving nodes share secret keys. Due to the wireless nature of the media and the unattended nature of sensor networks, it is extremely challenging to ensure authentication.

Data integrity in sensor networks is needed to ensure the reliability of the data and refers to the ability to confirm that a message has not been tampered with, altered or changed. Even if the network has confidentiality measures, there is still a possibility that the data integrity has been compromised by alterations. The integrity of the network will be in trouble when:

- A malicious node present in the network injects false data.
- Unstable conditions due to wireless channel cause damage or loss of data.

Availability determines whether a node has the ability to use the resources and whether the network is available for the messages to communicate. However, failure of the base station or cluster leader's availability will eventually threaten the entire sensor network. Thus availability is of primary importance for maintaining an operational network.

SECONDARY GOALS

Even if confidentiality and data integrity are assured, there is a need to ensure the freshness of each message. Informally, data freshness suggests that the data is recent and it ensures that no old messages have been replayed. To solve this problem a nonce, or another time related counter, can be added into the packet to ensure data freshness. A wireless sensor network is a typically an ad hoc network, which requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations. There is no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature brings a great challenge to wireless sensor network security. If self-organization is lacking in a sensor network, the damage resulting from an attack or even the risky environment may be devastating.

Most sensor network applications rely on some form of time synchronization. Furthermore, sensors may wish to compute the end-to-end delay of a packet as it travels between two pair wise sensors. A more collaborative sensor network may require group synchronization for tracking applications. Often, the utility of a sensor network will rely on its ability to accurately and automatically locate each sensor in the network. A sensor network designed to locate faults will need accurate location information in order to pinpoint the location of a fault. Unfortunately, an attacker can easily manipulate non secured location information by reporting false signal strengths, replaying signals.

SECURE DETECTION IN WIRELESS SENSOR NETWORKS

Wireless sensor networks (WSNs) are vulnerable to several types of attacks including passive eavesdropping, jamming, compromising of the sensor nodes and insertion of malicious nodes into the network [2]. Widespread adoption of WSNs, particularity for mission-critical tasks, hinges on the development of strong protection mechanisms against such attacks. Due to the scarcity of resources, traditional wireless network security solutions are not viable for WSNs. The life span of a sensor node is usually determined by its energy supply which is mostly expended for data processing and communication. Size and cost constraints of the nodes limit their memory size and processing power [12]. Therefore, security solutions which demand excessive processing, storage or communication overhead are not practical. In particular, due to their high computational complexity, public key ciphers are not suitable for WSNs.

An important application of WSNs, which has been extensively studied in recent years, involves decentralized detection whereby the sensors send their measurements to an ally fusion center (AFC) which attempts to detect the state of nature using the data received from all the sensors. Due to the broadcast nature of the wireless media, the sensors' data are prone to interception by unauthorized parties.

In this paper we are concerned with data confidentiality in the presence of passive eavesdropping. In particular, we assume that the transmissions of the nodes are over insecure

channels. An eavesdropping fusion center (EFC) is attempting to intercept the sensor's messages and to detect the state of nature. Since the sensors' data are used for hypothesis testing, security can be provided by degrading the detection performance of EFC. The communication between the sensors and AFC is assumed to be over a parallel access channel where the sensors are connected to AFC by a dedicated channel. The dedicated channels are assumed to be independent and identical and are modeled discrete memoryless channels (DMCs).

In [1], probabilistic ciphers were proposed as an easy solution to provide physical layer security for decentralized detection. This approach does not introduce any communication overhead for the sensors and has minimal processing requirements making it scalable in terms of network size. In this paper we revisit the problem of security in decentralized detection using WSNs. To protect their transmitted data from EFC, the sensors randomly alter their messages according to a secure stochastic matrix assigned to them prior to deployment. It is assumed that AFC is aware of the key used by each sensor. On the other hand, EFC, while aware of the encryption process and the set of keys, is unaware of which key is assigned to which sensor. Our goal is to achieve perfect secrecy at the physical layer by ensuring that the data observed by EFC is useless for detection purposes. We adopt J-divergence as the performance metric for both AFC and EFC and obtain the optimal solution for the cipher matrices so as to maximize AFC's divergence subject to zero divergence for EFC. As a result EFC will experience a poor detection performance. The cost of this perfect secrecy is a small deterioration in the detection performance of AFC. Since the detection error probability decays exponentially with the number of sensors, in a large network, the detection probability of AFC usually surpasses the design requirements. The proposed approach has minimal processing requirements and does not introduce any communication overhead.

ATTACKS ON SENSOR NETWORKS

Wireless Sensor networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected. Basically attacks are classified as active attacks and passive attacks.

PASSIVE ATTACKS

The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack. The Attacks against privacy is passive in nature. The main privacy problem is not that sensor networks enable the collection of information. In fact, much information from sensor networks could probably be collected through direct site surveillance. Rather, sensor networks intensify the privacy problem because they make large volumes of information easily available through remote access. Hence, adversaries need not be physically present to maintain surveillance. They can gather information at low-risk in anonymous manner. Some of the more common attacks against sensor privacy are:

In Traffic Analysis Even when the messages transferred are encrypted, it still leaves a high possibility analysis of the communication patterns. Sensor activities can potentially reveal enough information to enable an adversary to cause malicious harm to the sensor network. In Camouflage Adversaries One can insert their node or compromise the nodes to hide in the sensor network. After that these nodes can copy as a normal node to attract the packets, then misroute the packets, conducting the privacy analysis.

ACTIVE ATTACKS

The unauthorized attackers monitors, listens to and modifies the data stream in the communication channel are known as active attack.

ROUTING ATTACKS IN SENSOR NETWORKS

The attacks which act on the network layer are called routing attacks. The following are the attacks that happen while routing the messages. An unprotected ad hoc routing is vulnerable to these types of attacks, as every node acts as a router and can therefore directly affect routing information.

- Create routing loops
- Extend or shorten service routes
- Generate false error messages
- Increase end-to-end latency

SELECTIVE FORWARDING

A malicious node can selectively drop only certain packets. Especially effective if combined with an attack that gathers much traffic via the node. In sensor networks it is assumed that nodes faithfully forward received messages. But some compromised node might refuse to forward packets, however neighbors might start using another route

SINKHOLE ATTACK AND WORMHOLES ATTACKS

Attracting traffic to a specific node in called sinkhole attack. In this attack, the adversary's goal is to attract nearly all the traffic from a particular area through a compromised node. Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes. In the wormhole attack, an attacker records packet at one location in the network, tunnels them to another location and retransmits them into the network.

SYBIL ATTACKS

A single node duplicates itself and presented in the multiple locations. The Sybil attack targets fault tolerant schemes such as distributed storage, multipath routing and topology maintenance. In a Sybil attack, a single node presents multiple identities to other nodes in the network. Authentication and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network.

HELLO FLOOD ATTACKS

An attacker sends or replays a routing protocol's HELLO packets from one node to another with more energy. This attack uses HELLO packets as a weapon to convince the sensors in WSN. In this type of attack an attacker with a high radio transmission range and processing power sends HELLO packets to a number of sensor nodes that are isolated in a large area within a WSN. The sensors are thus influenced that the adversary is their neighbor. As a result, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbor and are ultimately spoofed by the attacker.

DENIAL OF SERVICE

Denial of Service (DoS) is produced by the unintentional failure of nodes or malicious action. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. In wireless sensor networks, several types of DoS attacks in different layers might be performed. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion and unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and de-synchronization. The mechanisms to prevent DoS attacks include payment for network resources, pushback, strong authentication and identification of traffic.

NODE LEVEL ATTACKS

Capture of a node may reveal its information including disclosure of cryptographic keys and thus compromise the whole sensor network. A particular sensor might be captured and information stored on it might be obtained by an adversary. A malfunctioning node will generate inaccurate data that could expose the integrity of sensor network especially if it is a data-aggregating node such as a cluster leader. Node outage is the situation that occurs when a node stops its function. In the case where a cluster leader stops functioning, the sensor network protocols should be robust enough to mitigate the effects of node outages by providing an alternate route.

PHYSICAL ATTACKS

Sensor networks typically operate in hostile outdoor environments. In such environments, the small form factor of the sensors, coupled with the unattended and distributed nature of their deployment make them highly susceptible to physical attacks, i.e., threats due to physical node destructions. Unlike many other attacks mentioned above, physical attacks destroy sensors permanently, so the losses are irreversible. For instance, attackers can extract cryptographic secrets, tamper with the associated circuitry, modify programming in the sensors, or replace them with malicious sensors under the control of the attacker. A false node involves the addition of a node by an adversary and causes the injection of malicious data. An intruder might add a node to the system that feeds false data or prevents the passage of true data. Insertion of malicious node is one of the most dangerous attacks that can occur. Malicious code injected in the network could

spread to all nodes, potentially destroying the whole network, or even worse, taking over the network on behalf of an adversary.

Conceptually, a node replication attack is quite simple; an attacker seeks to add a node to an existing sensor network by copying the node ID of an existing sensor node. A node replicated in this approach can severely disrupt a sensor network's performance. Packets can be corrupted or even misrouted. By inserting the replicated nodes at specific network points, the attacker could easily manipulate a specific segment of the network, perhaps by disconnecting it altogether. An adversary with powerful resources can collect information from the sensor networks if it is not encrypted. An intruder with an appropriately powerful receiver and well-designed antenna can easily pick off the data stream. Interception of the messages containing the physical locations of sensor nodes allows an attacker to locate the nodes and destroy them. Besides the locations of sensor nodes, an adversary can observe the application specific content of messages including message IDs, timestamps and other fields. To minimize the threats of passive information gathering, strong encryption techniques needs to be used.

PROBLEM STATEMENT

The wireless sensor network data collection process is carried out with reference to the query and request levels. The sensor node captures the data value and updates it into the local storage. The data values re transferred with reference to the request received by the node. The nodes here transmit their quantized observation and EFC is able to intercept the actual transmitted messages. While also use divergence as the performance measure for AFC and EFC, security is provided through probabilistic ciphers. Here an adversary inserts a number of malicious nodes into the network which deteriorate the detection performance by transmitting false data it is assumed that through collaboration, the Byzantine nodes are aware of the true hypothesis. It considers adding stochastic resonance noise at the honest in order to enhance the detection performance.

To reduce communication costs some algorithms remove or reduce nodes' redundant sensor information and avoid forwarding data that is of no use. As nodes can inspect the data they forward, they can measure averages or directionality for example of readings from other nodes. For example, in sensing and monitoring applications, it is generally the case that neighboring sensor nodes monitoring an environmental feature typically register similar values. This kind of data redundancy due to the spatial correlation between sensor observations inspires techniques for in-network data aggregation and mining. The following problems are identified from the current Wireless sensor Network security Scheme

- Scarcity of resources.
- Wireless network security solutions are not viable for WSNs.
- Due to their high computational complexity, public key ciphers are not suitable for WSNs.
- Data are prone to interception by unauthorized parties.
- The nodes are over insecure channels.

OPTIMAL BINARY DATA FUSION MECHANISM FOR WSN

The optimal solution for the cipher matrices is obtained in order to maximize J-divergence for AFC, whereas ensuring that it is zero for the EFC**.** Probabilistic ciphers were proposed as an easy solution to provide physical layer security for decentralized detection. This approach does not introduce any communication overhead for the sensors and has minimal processing requirements making it scalable in terms of network size. In this paper, revisit the problem of security in decentralized detection using WSNs. To protect their transmitted data from EFC, the sensors randomly alter their messages according to a secure stochastic matrix assigned to them prior to deployment.

It is assumed that AFC is aware of the key used by each sensor. On the other hand, EFC, while aware of the encryption process and the set of keys, is unaware of which key is assigned to which sensor perfect secrecy at the physical layer by ensuring that the data observed by EFC is useless for detection purposes. The cost of this perfect secrecy is a small deterioration in the detection performance of AFC. The proposed approach has minimal processing requirements and does not introduce any communication overhead for the sensors. The data gathered from wireless sensor networks is usually saved in the form of numerical data in a central base station.

If a centralized architecture is used in a sensor network and the central node fails, then the entire network will collapse, however the reliability of the sensor network can be increased by using distributed control architecture. Distributed control is used in WSNs for the following reasons: Sensor nodes are prone to failure, for better collection of data, to provide nodes with backup in case of failure of the central node. There is also no centralized body to allocate the resources and they have to be self organized. System Implementation has the following phases:

REFERENCES

[1]. M. Naraghi-Pour and V. Nadendla, "Secure detection in wireless sensor networks using a simple encryption method," in *Proc. IEEE WCNC*, Cancun, Mexico, Mar. 2011.

[2]. M. Orooji and M. Naraghi-Pour, "Decentralized hypothesis testing in wireless sensor networks in the presence of misbehaving nodes," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, Jan. 2013.

[3]. H. Jeon and J. Ha, "Cooperative secure transmission for distributed detection in wireless sensor networks," in *Proc. IEEE 54th Int. MWSCAS*, Seoul, Korea, Aug. 2011.

[4]. H. Jeon, J. Choi, S. McLaughlin and J. Ha, "Channel aware encryption and decision fusion for wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, Apr. 2013.

[5]. H. Jeon, J. Choi, H. Lee and J. Ha, "Secure type-based multiple access," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, Sep. 2011.

[6]. R. Soosahabi and M. Naraghi-Pour, "Scalable PHY-layer security for distributed detection in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, Aug. 2012.

[7]. Rawat, Chen and Varshney, "Collaborative spectrum sensing in the presence of Byzantine attacks in cognitive radio networks," *IEEE Trans. Signal Process.*, Feb. 2011.

[8]. F. Penna, Y. Sun, L. Dolecek and D. Cabric, "Detecting and counteracting statistical attacks in cooperative spectrum sensing," *IEEE Trans. Signal Process.*, 2012.

[9]. M. Abdelhakim, L. Zhang, J. Ren and T. Li, "Cooperative sensing in cognitive networks under malicious attack," in *Proc. IEEE ICASSP*, Prague, May 2011.

[10]. M. Gagrani, A. Vempaty, H. Chen, *et al.*, "On noise-enhanced distributed inference in the presence of Byzantines," in *Proc. 49th Annu. Allerton Conf. Commun., Control, Comput.*, Monticello, IL, USA, Sep. 2011.

[11]. M. Abdelhakim and T. Li, "Reliable data fusion in wireless sensor networks under Byzantine attacks," in *Proc. Mil. Commun. Conf.*, Baltimore, MD, USA, Nov. 2011.

[12]. Reza Soosahabi and Magdy A. Bayoumi, "Optimal Probabilistic Encryption for Secure Detection in Wireless Sensor Networks", IEEE Transactions On Information Forensics And Security, March 2014.