International Journal of Networking and Computing – www.ijnc.org
ISSN 2185-2839 (print) ISSN 2185-2847 (online)
Volume 7, Number 1, pages 50–68, January 2017

Strong Security Approach with Compromised Nodes Detection in Cognitive Radio Sensor Networks

Liang Hong
Department of Electrical and Computer Engineering, Tennessee State University
Nashville, TN, 37209, USA

Wei Chen
Department of Computer Science, Tennessee State University
Nashville, TN, 37209, USA

Sachin Shetty
Department of Modeling, Simulation and Visualization Engineering, Old Dominion University
Suffolk, VA, 23435, USA

Dan Lo
Department of Computer Science, Kennesaw State University
Kennesaw, GA, 30144, USA

and

Reginald Cooper
U. S. Air Force Research Laboratory
London, OH, 43140, USA

Received: July 25, 2016
Revised: November 22, 2016
Accepted: December 21, 2016
Communicated by Susumu Matsumae

Abstract

Cooperative MIMO communication is a promising technology which enables realistic solution for improving communication performance with MIMO technique in wireless networks that are composed of size and cost constrained devices. However, the security problems inherent to cooperative communication also arise. Cryptography can ensure the confidentiality in the communication and routing between authorized participants, but it usually cannot prevent the attacks from compromised nodes which may corrupt communications by sending garbled signals. In this paper, we propose a cross-layered approach to enhance the security in query-based cooperative MIMO sensor networks. The approach combines efficient cryptographic technique implemented in upper layer with a novel information theory based compromised nodes detection algorithm in physical layer. In the detection algorithm, a cluster of K cooperative nodes are used to identify up to $K-1$ active compromised nodes. When the compromised nodes are detected, the key revocation is performed to isolate the compromised nodes and reconfigure

the cooperative MIMO sensor network. During this process, beamforming is used to avoid the information leaking. The proposed security scheme can be easily modified and applied to cognitive radio networks. In such cognitive radio network, if we assume that in cooperative transmission the unlicensed users use one licensed user's frequency, a cluster of K cooperative nodes can identify up to $K-2$ active compromised nodes. Simulation results show that the proposed algorithm for compromised nodes detection is effective and efficient, and the accuracy of received information is significantly improved.

Keywords: cooperative MIMO radios, cryptography, beamforming, information theory, security of wireless communication

1 Introduction

Due to recent advances in electronics, wireless communications and computing technologies, wireless sensor networks (WSNs) have been widely deployed in many applications, including military sensing and tracking, environment monitoring, smart home appliances management, health-care, etc [1]. In WSNs, the sensor nodes may be remotely deployed in harsh environments, where reliable communication links are usually not available and each sensor node has to depend on its energy-limited battery for its operation. By exploiting spatial diversity with multiple antennas at the transmitter and receiver, the Multiple-Input Multiple-Output (MIMO) technique, which can provide significant increases in data rate and link range without additional bandwidth or transmission power, has attracted much attention in literature [2]. However, the physical implementation of multiple antennas at a small-size cost constrained node may not be feasible [3, 4, 5].

Recently, cooperative MIMO has been an emerging technique to achieve the benefits of the MIMO technique without the need of multiple antennas at each sensor node [6]. In cooperative MIMO WSNs, multiple single-antenna sensor nodes are physically grouped together to cooperatively transmit and/or receive. It has been proved that cooperative MIMO based sensor networks lead to better energy optimization and smaller end-to-end delay [7, 8].

The involvement of multiple nodes for transmission and/or receiving poses a challenge to the integrity of the information. Most schemes for traditional cooperative MIMO WSNs do not include considerations for potential security problems in communications at the design stage and are known publicly [9]. Therefore, attackers can easily launch attacks by exploiting security holes in those schemes. Cryptography can prevent some of the external attacks where the attacking nodes are not authorized participants of the sensor networks. However, in general, it cannot prevent the internal attacks from compromised nodes because these nodes can encrypt and decrypt the information. Therefore, compromised nodes can eliminate all the efforts to prevent attacks [10].

According to the operation mode, the attacks from compromised nodes can be passive or active [9]. The impact of active attacks is more severe than passive attacks since active attacks from just a few compromised nodes would make the entire network fail. The passive compromised nodes do not relay at all. The active compromised nodes will maliciously modify the relay information and inject falsified information. If there are active compromised nodes and the receiver treats them as trusted nodes, it will easily lead to symbol detection errors. Reference [11] elaborates the impact of the attacks from active compromised nodes and shows how easily the garbled information can lead to a failed data transmission through an example. The simulations in Section 7 will also illustrate this impact and show that the conventional WSNs without compromised nodes detection will fail due to the high bit error rate. Thus in subsequent discussions, we will focus on combating active attacks from the compromised nodes and ensure that the data from the source node can be delivered across the network securely.

A variety of techniques have been proposed to secure the communication in WSNs. In [12, 13], the threats and vulnerabilities to WSNs, security requirements, and secured communication solutions are summarized. Cryptography based approaches, either using public key cryptography or using symmetric key cryptography, are widely used to secure the communication in WSNs [9, 14, 15]. For the WSNs of small sized sensor nodes, symmetric key cryptography is more time and energy efficient. On the other hand, secured communication techniques in physical layer are more promising, since they can be more effective in resolving the boundary, efficiency, and link reliability issues [16]. [16]

and [17] exploited signal randomization to effectively scramble the eavesdropper's signals but not the authorized receiver's signals. In [18] the security of communications is enhanced by adding artificial noise to the transmission process in the physical layer with extra MIMO antennas. Their scheme assumes a key management system in a higher layer and the artificial noise is generated by the keys shared with neighboring nodes. However, none of these schemes detects and defends against node compromise. Moreover, all these schemes need extra MIMO antennas to achieve data assurance, which largely reduces the advantage of MIMO technique. Mao and Wu proposed a cross-layer scheme that uses pseudo-random tracing symbols at the physical layer and direct sequence spread spectrum symbols at the application layer for tracing and identifying the compromised nodes [11]. However, this scheme increased the overhead and power consumption of the transmission and reduced the throughput due to the tracing symbols insertion and tracking.

In [19, 20, 21], we investigated a secured communication scheme in cross layered manner for cooperative MIMO networks. The scheme combines a cryptographic technique implemented in higher layers and data assurance analysis at the physical layer. An efficient key management system is used for cryptography to ensure data confidentiality, message authentication and etc. It provides secured communication and routing using a small number of keys shared between the clusters cooperating on data transmission and reception. The situation where some cooperative nodes are compromised and try to corrupt the communications by sending garbled signals is also investigated. An information theory based approach is used at the physical layer to identify the compromised nodes in a cooperative cluster A by one of its neighboring cluster D. In [21], the number of detectable compromised nodes is maximized to one third of the smaller number of nodes in clusters A and D. The corrupted symbols can be also recovered in transmission process at physical layer.

In this paper, by taking into account a query-based information collection application, we substantially improve the above scheme by proposing a novel detection algorithm that can identify all compromised nodes in a cooperative cluster if the number of compromised nodes is less than the number of nodes in the detecting cluster. When the compromised nodes are detected, beamforming is used to prevent information leaking during the process of the key revocation and network reconfiguration. Simulation results show that the proposed algorithm for compromised nodes detection is effective and efficient, and the accuracy of received information is significantly improved. Comparing with the existing schemes in [9-18], our proposed scheme detects and defends against compromised nodes without the need for extra MIMO antennas or the tracing symbols. Moreover, the proposed scheme requires much smaller number of pre-loaded keys for key establishment and prevents the compromised nodes to pretend to be trustworthy nodes. Furthermore, by adjusting the security level, the proposed scheme can achieve different tradeoffs between energy and communication efficiency and the integrity of the received data. In [21], it is assumed that every cluster contains more than half non-compromised nodes. The detector D can identify all active compromised nodes in a cooperative cluster A when the number of active compromised nodes in A is less than $\min(|A|, |D|)/3$, where $|x|$ stands for the number of nodes in cluster x and min stands for the smaller value. Comparing with [21], the detector D in this work can identify all active compromised nodes in A if the number of active compromised nodes in A is less than $|D|$. Moreover, by using beamforming, the transmission towards the compromised nodes can be nulled out and information leaking can be stopped immediately, while in [21] the information leaking cannot be prevented until the key management system completes the process of key revocation to isolate the compromised nodes and reconfigure the cooperative MIMO network.

Cognitive radio is a promising paradigm for wireless communications that enables efficient use of frequency resources by allowing the coexistence of licensed primary users and unlicensed secondary users in the same frequency band. The proposed security scheme can be easily modified for cognitive radio network by using the same beamforming technique to avoid interference to the licensed user. If we assume that the unlicensed secondary users use one licensed primary user's frequency to do cooperative data transmission, a cluster of K cooperative nodes in such cognitive radio network can identify up to $K-2$ active compromised nodes.

The primary results in this paper was presented in [22]. In this paper, the strong security approach is generalized into cognitive radio sensor networks. Furthermore, more simulations are conducted and explanations are given to accommodate the scenarios for cognitive radio networks.

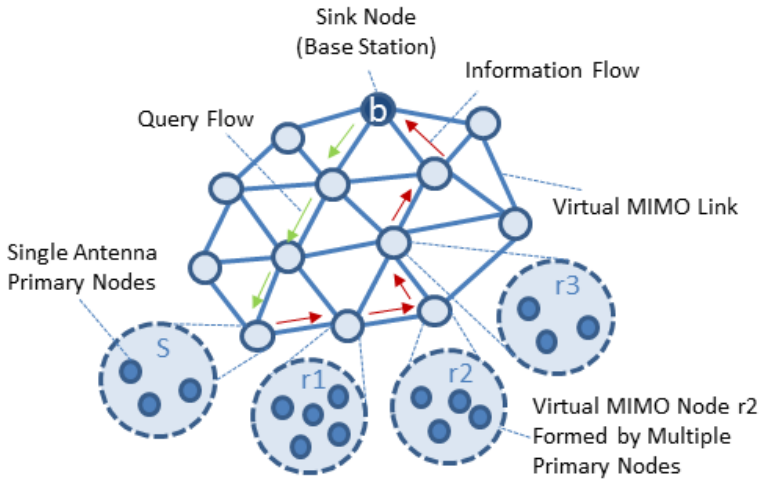

Figure 1: System model

The rest of this paper is organized as follows. Section 2 briefly describes the system model, beamforming technique, and framework of the proposed cross-layered secured communication scheme. Section 3 shows cooperative communication and relay scheme. Section 4 presents compromised nodes detection, symbol recovery, and information leaking prevention schemes. Section 5 states the security key management scheme with key revocation and network recovery. Section 6 shows how to apply the proposed security scheme to cognitive radio network. Section 7 shows the performance of the proposed secured communication scheme for cooperative MIMO networks through computer simulations. Finally, a conclusion is drawn in Section 8.

2 System Model, beamforming, and framework of secured communication scheme

2.1 System Model

In this paper, a multi-hop cooperative wireless sensor network that relays the source data from a source node to the sink node (base station) based on the query issued by the sink node is considered. As shown in Figure 1, the WSN consists of a set of sensor nodes that are equipped with a single-antenna radio. These single-antenna nodes are called primary nodes. Information collected by local sensors needs to be aggregated and relayed to a remote sink. The sensor nodes will form into clusters and serve as relay nodes to improve the communication quality by using the benefit of the MIMO technique. These clusters are also called virtual MIMO nodes in the rest of the paper, such as nodes S, $r1$ in Figure 1. The transmission link between two virtual MIMO nodes is called virtual MIMO link. The sink node b can be a virtual MIMO node or a node equipped with multiple antennas. It sends a request to the source cluster S, and then the primary nodes in S cooperatively send source information which are collected in S back to sink node.

Among the cooperative strategies, the amplify-and-forward and decode-and-forward are most widely used. In the amplify-and-forward strategy, the relay nodes simply boost the energy of the signal received from the sender and retransmit it to the receiver. In the decode-and-forward strategy, the relay nodes will perform physical layer decoding (signal detection and demodulation) and then forward the decoded results. Although the amplify-and-forward relay has lower relay power consumption, it also amplifies the noise in the received signal and is not suitable for long-haul transmission. Moreover, decoding may be necessary when data aggregation and/or fusion is required at some local points such as cluster heads. Furthermore, considering that the decode-and-forward relay can be extended to combine with coding techniques and is easier to incorporate into network

protocols [23], it will be considered in this paper.

Consider that the transmitting and receiving clusters have m_T and m_R nodes, respectively, the received signal at the virtual receiving MIMO node can be represented as [24]

$$\mathbf{y} = \mathbf{H}\mathbf{s} + \mathbf{n}, \tag{1}$$

where $\mathbf{y} = [y_1, y_2, \cdots, y_{m_R}]^T$ is a $m_R \times 1$ vector representing the received signals at the receiving cluster, $\mathbf{s} = [s_1, s_2, \cdots, s_{m_T}]^T$ is a $m_T \times 1$ vector representing the transmitted signal at the transmitting cluster, $\mathbf{H}$ is the a $m_R \times m_T$ matrix of channel coefficients, $\mathbf{n} = [n_1, n_2, \cdots, n_{m_R}]^T$ is a $m_R \times 1$ vector representing the additive Gaussian noise components, they are identically distributed and mutually statistically independent, each having zero mean and two-sided power spectral density $2N_0$.

Since this paper focused on ensuring the security of communications in a cooperative MIMO network, we assume that the channel matrix $\mathbf{H}$ is known. This is feasible and can be achieved by using proper channel estimation method that is performed frequently enough to track the channel variations [25, 26]. Usually the channel estimation is based on the known sequence of bits, which is unique for a certain transmitter and which is repeated in every transmission burst. Thus, the channel matrix $\mathbf{H}$ can be estimated for each burst separately by exploiting the known transmitted bits and the corresponding received samples.

2.2 Beamforming Technique

Beamforming is a signal processing technique for directional signal transmission or reception [27]. It is achieved by combining elements in a phased array of antennas in such a way that signals at particular angles experience constructive gains while others experience destructive interferences. Beamforming is widely used in cognitive radio networks. In order to avoid the interference, the cognitive users use beamforming to pose null constraints to the licensed users.

Cooperative MIMO can largely benefit from multiple cooperative antennas to limit or avoid interference towards the primary nodes or prevent the information leaking to the adversary nodes by pose the null constraints. Theoretically, a k-antenna transmit beamformer can form h $(1 \leq h \leq k)$ constructive beams and null out $k - h$ directions simultaneously. In the proposed scheme, when the compromised nodes are detected, key renovation and cluster reconfiguration will be invoked. During this process, information leaking is avoided by using the beamforming technique.

2.3 Framework of Cross-Layer Secured Communication Scheme

The proposed cross-layer secured communication scheme for cooperative MIMO networks is shown in Figure 2. Based on the security level set by the sink, each of the primary nodes in the receiving/detection process will determine whether it needs to perform compromised nodes detection during the sink defined time period. If detection is not needed, normal cooperative data transmission or relay will be conducted during this time period. Otherwise, compromised nodes detection will be performed. If the detection results indicate that there is no compromised node, normal cooperative data transmission or relay will be conducted for the rest of the time period. Otherwise, symbol recovery will be conducted to eliminate the garbled symbol, and beamforming is used to pose null constraints to the compromised nodes for information leaking prevention. The detection report will also be sent to the sink and normal cooperative data transmission or relay will be conducted for the rest of the time period. On the other hand, if the sink receives the report of compromised nodes, the key management system will invoke the key revocation to maintain the accuracy of the next detection and stop compromised nodes getting information from the network and reconfigure the cooperative MIMO network. Then all nodes in the detection cluster go back to the normal communication.

To operate the proposed cross-layered secured communication scheme, there are three major tasks: 1) how to form the cooperative MIMO network with distributed primary nodes and cooperatively transmit information; 2) how to detect the compromised nodes; and 3) how to establish secret

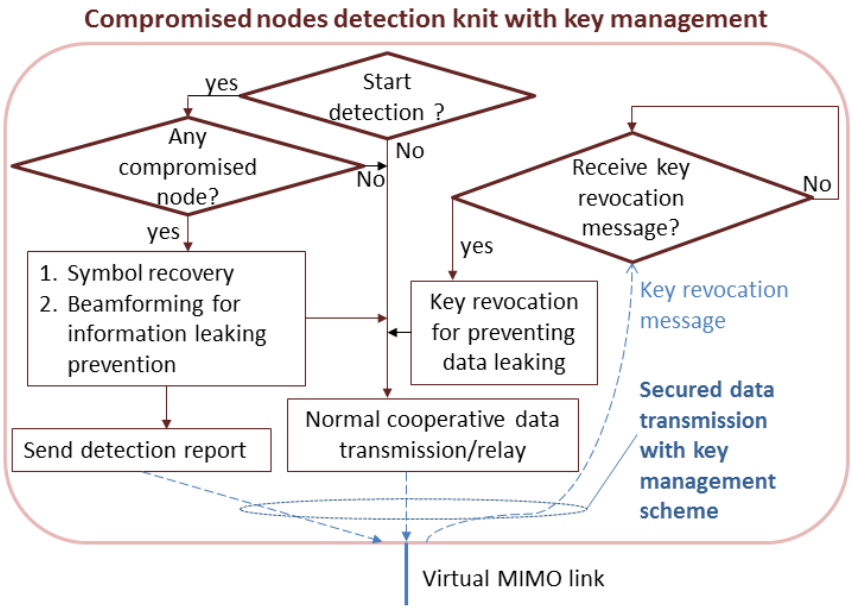

Figure 2: Cross-layer secured communication scheme for cooperative MIMO networks

key and build secured communication and routing. The accomplishments of these three tasks are presented in the next three sections.

3 Cooperative Network Architecture and Data Transmission Scheme

3.1 Cooperative MIMO Networking Architecture and Formation

Let G be a network of single-antenna wireless nodes and V be the set of nodes in G. A d-clustering of V is a node-disjoint division of V, where the distance of two nodes in a d-cluster is not larger than d. Let A and B be two d-clusters. If the distance of any node of A and any node of B does not exceed $D(D >> d)$, a D-$m_T \times m_R$ cooperative MIMO transmission link can be defined between A and B, where m_T=$|A'|$ and m_R=$|B'|$, A' and B' are the subsets of A and B. Let the nodes in A' and B' are ordered by their IDs. The ith node in A' uses its antenna as the ith antenna cooperating the transmission and the jth node in B' uses its antenna as the jth antenna cooperating the reception. In order to avoid confusion, in this paper, a single-antenna wireless node in G is called as *primary node*, a d-cluster is called as *virtual MIMO node*, and a D-$m_T \times m_R$ cooperative MIMO transmission link is called as *virtual MIMO link*. Given d and D, a cooperative MIMO (CMIMO) radio network of G can be represented by an undirected graph $G_{CMIMO} = (V_{CMIMO}, E_{CMIMO})$, where V_{CMIMO} is the set of the d-clusters, and E_{CMIMO} is the set of edges. An edge $(A, B) \in E_{CMIMO}$ if and only if $A, B \in V_{CMIMO}$ and there is a D-$m_T \times m_R$ cooperative MIMO link between A and B. A cooperative MIMO network can be formed from the given G, d, and D as follows [8]:

1. the primary nodes in G self-form a cooperative MIMO radio network G_{CMIMO} by using a distributed clustering algorithm on G,

2. the virtual MIMO nodes (d-clusters) form a backbone tree by using a distributed Spanning-Tree formation algorithm on G_{CMIMO}, and

3. the routing for data dissemination, data gathering and unicast is constructed by the paths of the backbone tree.

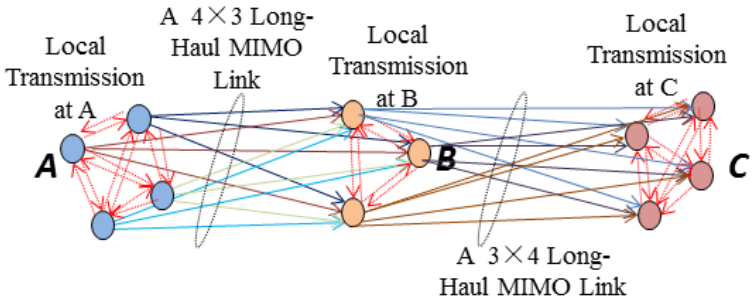

Figure 3: Cooperative MIMO data transmission scheme

After the CMIMO network formation, each cluster A has a cluster ID. Each primary node in A retains the following information: ID of cluster A, IDs of all primary nodes in A, IDs and sizes of the clusters in two hops of A in the backbone tree. If considering the case that one node may move in or move out of the network (e.g., the node leaves the network when its battery level is lower than the threshold and it comes back when the battery is recharged, or the node is mobile), the reconfiguration of the network may be required. This is not the subject of the paper. The corresponding reconfiguration algorithms can be found in [8].

3.2 Cooperative Data Transmission Scheme

We consider a cooperative MIMO data relay. There are two types of communication in a cooperative MIMO relay network: local/intra communication at virtual MIMO nodes and long-haul/inter communication between virtual MIMO nodes [3, 28]. The following MIMO scheme cooperatively relays $k(k \geq 1)$ data from a cluster A to a destination cluster, where A can be the base station when it sends a query to the source cluster or the source cluster when it sends the source data back to the base station:

MIMO Scheme for data relay between virtual nodes A and B

1. First hop between virtual nodes A and B (Figure 3) :

   It includes local transmission in virtual node A, and long-haul transmission between virtual nodes A and B:

   Step1 (Local transmission at A): Each primary node i in A with data I_i broadcasts its data to all other nodes using different timeslots. After this step, each node in A has data sequence $I = I_1, I_2, \cdots, I_k$.

   Step 2 (long-haul/cooperative transmission between A and B using multiple $m_T \times m_R$ MIMO link): Let $|A|$ and $|B|$ be the numbers of cooperative nodes in transmission side A and in reception side B, respectively. All nodes in B join cooperative reception, i.e., $m_R = |B|$. m_T nodes in cluster A are self-selected in turn to join cooperative transmission. The node with the ith smallest ID in the m_T nodes acts as the ith antenna and encodes the data sequence I using $m_T \times m_R$ MIMO coding. The selected m_T nodes in A broadcast encoded sequence I to the nodes in B at the same time. Each node in B receives combined m_T encoded sequences $\mathbf{y}$, where $\mathbf{y} = \mathbf{Hs} + \mathbf{n}$ and $\mathbf{s} = \{I, I, ..., I\}$ according to the system model in Section 2.
   m_T is decided as follows:
   m_T=min(a, b), where $a = \min(|PreA|, |A|, |PostA|)$, $b = |PreA| - K$, $PreA$ and $PostA$ are the clusters before and after A in the data relay route, respectively, and K is the largest possible number of compromised nodes in A.
   When m_T is smaller than $|A|$, the nodes in A transmit the data in turn, i.e., first the nodes with ith $(1 \leq i \leq m_T)$ smallest ID in A join the cooperative transmission, second, the nodes with the jth $(m_T + 1 \leq j \leq 2m_T)$ smallest ID in A join the transmission, and so on. Detailed

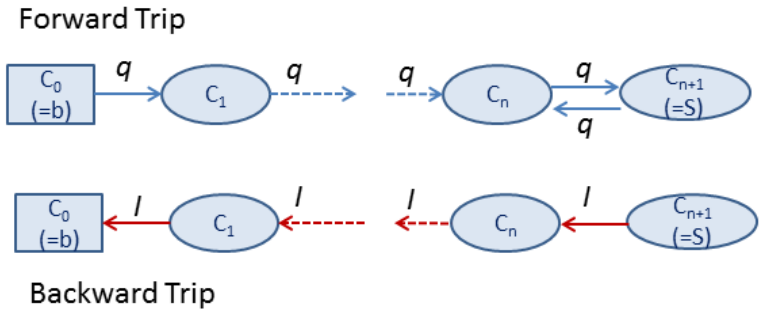

Figure 4: Compromised nodes detection process in a query-based application

derivation for condition of m_T is given in Section 4. Since each node in A has the list of IDs of the primary nodes in A and knows the sizes of A's neighboring cluster, it can calculate m_T, and judge if it should attend the data transmission.

Step3 (Local transmission at B): (i) Each primary node in B broadcasts the received data to all other primary nodes using different timeslots. (ii) After receiving the data from the other primary nodes, each primary node in B decodes the received data back to the original data sequence I.

2. Other hops between virtual nodes B and C

   This transmission consists the long-haul transmission between virtual nodes B and C that is similar to Step 2 in the first hop and the local transmission at C that is similar to Step 3 in the first hop. The only change is to replace A and B to B and C, respectively.

In [8] and [28], the cooperative transmission schemes using SIMO, MISO, and MIMO links are investigated. Comparing with the traditional SISO transmission scheme, the cooperative schemes can fully use the benefit from the diversity gain of antenna arrays and largely improve energy efficiency and network lifetime and reduce the transmission latency.

4 Compromised Nodes Detection with Information Recovery

In this Section, a round-trip process for compromised nodes detection in a query-based application is explained first, then the detailed compromised nodes detection scheme is elaborated. The scheme consists of two algorithms: one is for invoking a detection and the other is for detecting the compromised nodes. Based on the detection results, the symbol recovery method is used to eliminate the impact of the compromised nodes; a cooperative beamforming based method is used to prevent the information leaking to the compromised nodes. Figure 4 shows the compromised nodes detection process in a query-based application. Figure 5 shows the proposed compromised nodes detection scheme and the cooperative beamforming based information leaking prevention.

4.1 Compromised Nodes Detection Process in a Query-Based Application

Let the route from sink node b to source cluster S in the network is $C_0(=b)$, C_1, $\cdots$, C_{n-1}, C_n, $C_{n+1}(=S)$, where C_i, $i = 0, 1, \cdots, n+1$ is the clusters in the network. Detection is performed in the round trip from b to S and S to b as follows:

1. Forward trip

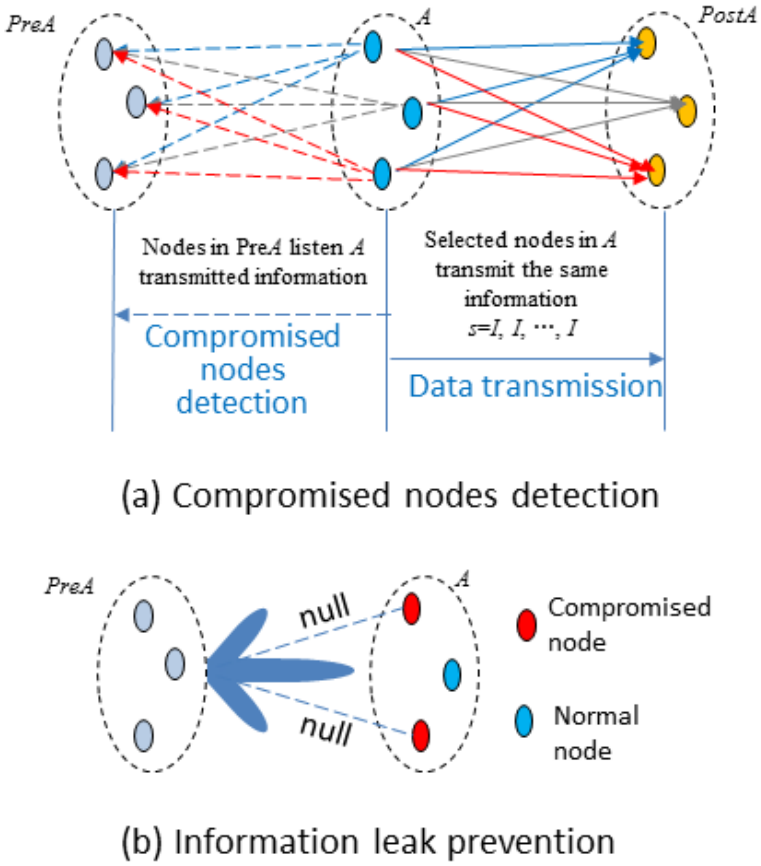

Figure 5: Compromised nodes detection and information leaking prevention

C_i transmits query request q to C_{i+1} for i from 0 to n, and then $C_{n+1}(= S)$ transmits q back to C_n. In this relay process, C_i detects C_{i+1} by listening when C_{i+1} transmits q to C_{i+2} for i from 0 to $n-1$, and C_n detects S when S transmit q back to C_n.

2. Backward trip

   C_i transmits source information I to C_{i-1} for i from $n+1$ down to 1, where $C_{n+1} = S$ and $C_0 = b$. In this relay process, C_i detects C_{i-1} by listening when C_{i-1} transmits I to C_{i-2} for i from $n+1$ down to 2.

4.2 Compromised Nodes Detection Scheme

Before we present the distributed algorithm for compromised nodes detection, we propose the following algorithm to determine at each cluster whether the compromised nodes detection is needed. In this algorithm, the sink broadcasts a time interval t_I, security level $0 \leq sl \leq 1$ and largest possible number K of compromised nodes in a cooperative cluster at the beginning of the WSN deployment. It may broadcast the adjusted t_I, sl, and K during the operation of the WSN when necessary. The shorter the time interval or the lower the security level, the more compromised nodes detections will be performed.

Algorithm: Start detection at cluster D?

1. At the beginning of each time interval t_I, the random number generator at the node h with the smallest ID in the cluster D generates a uniformly distributed random number l between

0 and 1.

2. h compares l with the sink defined security level.
3. If $l > sl$
   (a) Node h broadcasts the detection message to other nodes in the cluster D
   (b) D detects the compromised nodes in $PostD$ (the cluster after D in the relay route) through listening the signals that $PostD$ transmits to $PPostD$ (the cluster after $PostD$) using $\lceil |PostD|/m_T \rceil$ rounds, where m_T is the number of nodes in $PostD$ cooperating on data transmission. The nodes in D perform compromised nodes detection in this time interval.
4. Else No detection. The clusters perform normal cooperative data transmission or relay operation.

After the cluster decides that the compromised nodes detection is needed, the cluster will use symbols of time span t_d for detection, where $t_d << t_I$. The starting point of t_d is uniformly distributed in the sink defined time interval t_I.

Remarks:

1. In this proposed scheme, a cluster A relays data from $PreA$ to $PostA$. Cluster $PreA$ is used as the detector to identify the compromised nodes in A through listening signals when A relays the data to $PostA$. The detection is conducted at random times, the compromised nodes in a transmitting cluster do not know when to pretend to be trustworthy nodes. If the compromised nodes always pretend to be trustworthy nodes by transmitting correct data, they are not considered to be compromised nodes because all the data they transmitted are correct.
2. Detecting the compromised nodes at random times has two advantages. First, in the fixed-time detection scheme [19], the compromised nodes can pretend to be trustworthy nodes by sending the correct data only at the detection time. However, in this proposed scheme, they are not able to do it since they do not know when the detection process will be performed. Second, the security level is adapted according to the detected number of compromised nodes, so that the energy and communications of the whole WSN can be saved.
3. By using security level sl, unnecessary detection can be avoided. Therefore, time and power consumption can be reduced.

In multi-hop WSNs, except the sink node $C_0(= b)$, any one of the clusters will serve as the cluster to-be-detected when it is selected as relay cluster by the routing scheme. Consider any two consecutive clusters $PreA$ and A, where cluster $PreA$ is the cluster for detecting compromised nodes in cluster A. If there are compromised nodes in $PreA$, $PreA$ may detect the compromised nodes in A with higher error rate. However, these compromised nodes will be detected by the cluster $PPreA$ before $PreA$ and removed from $PreA$ with key revocation in the ($PPreA$, $PreA$) detection pair. After this, $PreA$ will not have compromised nodes and can detect compromised nodes in A with high accuracy. It is reasonable to assume that the sink node, $C_0(= b)$, is free of compromised nodes. Therefore, without loss of generality, in the following algorithm for compromised nodes detection, we assume that the detection cluster does not have compromised node.

As described in the MIMO transmission scheme, the m_T primary nodes in A transmit the same data, that is, $\mathbf{S} = \{I, I, ..., I\}$, to $PostA$. The primary nodes in $PreA$ receive the symbols through listening. When the detection is needed, the node p with the smallest ID in $PreA$ requests all the nodes in its cluster to broadcast the received symbols at different time slots. After local broadcast, each primary node in $PreA$ has received a complete data sequence $\mathbf{y}$ and will perform distributed detection to identify compromised nodes in cluster A. The following describes the compromised nodes detection algorithm:

Compromised nodes detection algorithm

According to the MIMO transmission scheme in Section 3, from the second hop m_T nodes of A in

turn (from the smallest ID) cooperate the data transmission to $PostA$. All nodes in A attend at least once data transmission in $\lceil |A|/m_T \rceil$ rounds. $PreA$ detects the compromised nodes in A during the same rounds. Let $\mathbf{H_i}$ $(1 \leq i \leq \lceil |A|/m_T \rceil)$ be the matrix of channel coefficients in the ith round. According to the system model in Section 2, it is assumed to be known to the detection cluster.

for round $i = 1$ to $\lceil |A|/m_T \rceil$ do the following steps:

1. After receiving complete data sequence $\mathbf{y}$ though listening, each primary node in the detection cluster $PreA$ performs Inverse Channel Detection [24] to estimate the transmitted symbols s. The inverse channel detector multiplies a weighting matrix that is inverse or pseudo-inverse of the channel matrix $\mathbf{H_i}$ with the received symbols to estimate the transmitted symbols s, that is, $\hat{\mathbf{s}} = \mathbf{W_i}^H \mathbf{y}$, where $\mathbf{W_i}$ is an $|PreA| \times m_T$ weighting matrix, and $(\cdot)^H$ represents Hermitian transpose. Since $m_T \leq |PreA|$ according to the condition of m_T in the MIMO transmission scheme, $\mathbf{W_i}$ can be determined by

$$\mathbf{W_i} = \begin{cases} \mathbf{H_i}^{-1}, & \text{if } m_T = |PreA| \\ (\mathbf{H_i}^H \mathbf{H_i})^{-1} \mathbf{H_i}^H, & \text{if } |PreA| \leq m_T \end{cases}$$

2. Based on the assumption that the symbols transmitted from A to $PostA$ (listened by $PreA$) by the non-compromised nodes should be the same as the ones $PreA$ sent to A, each node in $PreA$ can identify the compromised nodes x_i (if any) if in $\hat{\mathbf{s}}$=$\{\hat{s}_1, \hat{s}_2, ..., \hat{s}_{m_T}\}$ $\hat{s}_i \neq I$, and record their IDs.

3. For each primary node u in $PreA$, if it detected compromised nodes in A, it sends an encrypted detection report with a plain message (u's ID, the sink's ID, list of compromised nodes' IDs) and an encrypted message (u's ID, the sink's ID, list of compromised nodes' IDs) to the sink. If the sink receives the reports from all nodes of $PreA$ with the same list of compromised nodes' IDs, it can classify that the reports are true.

Remarks:

1. Comparing with [11], no tracing symbols are needed in the proposed compromised nodes detection algorithm, therefore, the proposed algorithm does not have the overhead and the system complexity is lower.

2. Comparing with [21], since the nodes in the detection cluster know what the correct data should be, decision in this work does not need to be made based on majority rule.

3. The proposed algorithm for compromised nodes detection will also work well when the space-time code is used. In this case, the symbol-by-symbol comparison will be replaced by the pattern comparison, where each pattern that includes several symbols is determined by the selected space-time code. Therefore, the full MIMO benefits can still be maintained with the proposed algorithm.

In the above proposed algorithm for compromised nodes detection, the largest possible number K of compromised nodes in A can be decided by the condition

$$m_T = \min(\min(|PreA|, |A|, |PostA|), |PreA| - K)$$

in the MIMO transmission scheme in Section 3.

Recall that m_T is the number of the nodes in A which cooperate on data transmission, all nodes of $PostA$ cooperate on reception and all nodes of $PreA$ cooperate on listening. The first part of condition m_T=$\min(|PreA|, |A|, |PostA|)$ is used to guarantee that the reception nodes in $PostA$ and listening nodes in $PreA$ are not less than the transmission nodes in A. The second part of the condition $m_T \leq |PreA| - K$ is used to guarantee that the total transmission nodes in A is not more than the listening nodes in $PreA$ even when K compromised nodes join the transmission. From the condition we have $K \leq |PreA| - m_T$. Therefore, K can be as large as $|PreA| - 1$ when $m_T = 1$.

4.3 Symbol Recovery and Leaking Prevention

When the compromised nodes in A are detected by $PreA$, all primary nodes in $PreA$ will form a detection report. All reports will be relayed from A to $PostA$, and finally relayed to the sink. If the list of compromised nodes from all nodes of $PreA$ are the same, the list can be trusted. As we mentioned in system model, $PostA$ decodes the received signals. Therefore, it can identify the signals that each node of A sent. If the message is sent from $PreA$, $PostA$ will decrypt the message and gets the list of the compromised nodes in A. Then $PostA$ will decode the data by simply setting the columns in channel matrix that corresponds to the compromised nodes to zero. This will eliminate the use of the malicious data by ignoring the symbols transmitted from the compromised nodes. Also, the nodes in $PreA$ will use beamforming immediately to block the symbols leaking to the compromised nodes. According to the beamforming technique in Section 2, up to $|PreA| - 1$ compromised nodes in A can be blocked from receiving the data.

Moreover, when the sink received the detection report, it will start the key revocation and network recovering process to prevent compromised nodes from getting information in the network (see Section 5). Then, all nodes in $PreA$ will stop the beamforming and go back to normal data transmission.

5 Security Key Management Scheme

The approach of key management in the section is almost the same as that in [21]. For the completeness, we describe it briefly here. The key management system is based on shared/symmetric key cryptography. It only needs a small number of pre-loaded keys. Since localization itself is a very challenging problem, the key establishment in this work uses topology knowledge instead of the location knowledge used in some existing work [29].

Types of keys: There are two types of keys used in the cooperative MIMO communications. They are:

- Shared keys, C-key(A), for local communication at each cluster.
- Shared keys, L-keys(A, B), for long-haul communication at each link of two clusters A and B in the backbone tree. When the primary nodes in A and B cooperate data transmission and reception, each node in A uses L-key(A, B) to encrypt the transmission data and each node in B uses the same key to decrypt the received data.
- Shared keys, D-key(A, C), for information recovery at each pair of two clusters A and C, where C is two hops away from A in the backbone tree.

Key pre-distribution: for each primary node u in WSNs, a shared key, pre-key(b, u), is pre-distributed at the sink b and at the node u, respectively.

Key establishment: The following algorithm is used for key establishment.

Key Establishment Algorithm (Assume that the CMIMO network is already formed):

1. A special node u (e.g., the primary node with the smallest ID) at each cluster A sends a key request to the sink b with a plain message (u's ID, b's ID) and an encrypted message (u's ID, b's ID, u's member-list of the cluster, u's neighbor-list of the backbone) encrypted by using pre-key(u, b).
2. When b receives the key request from u, b decrypts the message by using pre-key(b, u). After b receives the key requests from all clusters, it has the topology of the backbone tree in cooperative MIMO network. Then, b generates a C-key(A) for each cluster A, an L-key(A, B) for each A's neighbor B, and a D-key(A, C) for each cluster C which is two hopes from A in the backbone. b disseminates the key response to each primary node x in cluster A as follows: a plain message (b's ID, x's ID) and an encrypted message (b's ID, x's ID, C-key(A), a list of L-key(A, B), a list of D-key(A, C)) encrypted by pre-key(b, x).

3. When primary node x receives a key response, x decrypts the message by using pre-key(x, b) to get C-key, L-keys, and D-keys.

Remark:

When b disseminates the key response to a primary node x in cluster A, it delivers a package to x which includes the plain message (b's ID, x's ID) and an encrypted message (b's ID, x's ID, and a list of L-key(A, B), and D-key(A, C)). The key responses for n primary nodes are distributed by performing depth-first travel on the backbone tree of the CMIMO network. Due to the cooperative communication, when a virtual MIMO node on the backbone tree receives a key response, all primary nodes in the virtual node receive the same key response but only x can decrypts it. By using the pipeline manner, the time required for key distribution is $O(n+t)$, where n is the number of primary nodes, and t is the size of the backbone tree (i.e., the number of the clusters). The number of different keys required in the key management system is less then $4t$, where the number of C-keys is t, the number of L-keys is $t-1$, and the number of D-keys is no more than $3t$. Note that usually t is much smaller than n. After key establishment, each primary node u has C-key, L-keys, and D-keys. The number of keys is small and affordable for small and inexpensive nodes.

Secured Communication and Routing:

After the key establishment, the communication in each local virtual MIMO node A uses C-key(A) and in link AB at the backbone uses L-key(AB). Since the routing uses the paths on the backbone tree, cooperative data relay is secured.

The proposed key management system is more efficient than other existing systems: it uses shared/symmetric key cryptography which requires small size of keys, it needs only a small number of keys at each primary nodes, and key establishment can be performed without location knowledge.

5.1 Key Revocation and Network Recovering

If the sink receives the report of the compromised nodes in cluster A, it will start the key revocation and network recovering process. This approach is used to prevent compromised nodes from getting information in the network and sending false reports.

In key revocation, the sink b takes the following actions for key revocation and network recovery:

1. The sink b sends all nodes v in cluster A other than the compromised nodes a key revocation information with a plain message (b's ID, v's ID) and an encrypted message (b's ID, v's ID, new C-key(A), and ID list of the compromised nodes) encrypted by pre-key(b, v),

2. for each A's neighbor and its neighbor's neighbor (i.e., two hops from A) B in the backbone tree, b sends each node v in A (other than the compromised nodes) and in B a key revocation information with a plain message (b's ID, v's ID) and an encrypted message (b's ID, v's ID, new L-key(A, B), new D-key(A, B)) encrypted by pre-key(b, v).

3. When node v in A and B receives a key revocation information, it decrypts the message by pre-key(v, b) and gets a new C-key, new L-keys and new D-keys. In this way, the C-key for local communication in virtual node A, the L-keys for long-haul communication and the D-keys for information recovery are revoked. The compromised nodes do not have the new keys and will be not able to get information from the network.

6 Applying Proposed Security Scheme in a Cognitive Radio Network

Cognitive radio is a promising paradigm for wireless communications that enables efficient use of frequency resources by allowing the coexistence of licensed primary users and unlicensed secondary users in the same frequency band. The proposed security scheme in this paper can be easily modified and applied to a cognitive radio network by using the beamforming technique to avoid interference to the licensed primary user. In the data relay scheme in Section 3, m_T is the number of nodes in a

cluster cooperating on data transmission. Assume that they use a licensed primary user's frequency band, according to the beamforming technique in Section 2, a k-antenna transmit beamformer can form h ($1 \leq h \leq k$) constructive beams and null out $k-h$ directions simultaneously. Therefore, when null out the direction of the licensed primary user, $m_T - 1$ ($m_T \geq 2$) nodes can cooperate on data transmission. Let K be the number of compromised nodes in a cluster, in data relay, the compromised nodes in a cluster A can be detected by cluster $PreA$. According to the detection algorithm in Section 4, $K \leq |PreA| - m_T$, K can be as large as $|PreA| - 2$ when $m_T = 2$. Therefore, $PreA$ can detect up to $|PreA| - 2$ compromised nodes in A.

7 Simulation Results

In this section we investigate the performance of the proposed compromised nodes detection algorithm and the cooperative secured communication system through computer simulations using MATLAB. In the simulations, multiple single-antenna sensor nodes are physically grouped together to form a cooperative MIMO system. The active compromised nodes attack is considered. Since $PreA$ is used to detect compromised nodes in A and knows which information should be transmitted by nodes in A, without loss of generality, the compromised nodes are assumed to transmit randomly generated symbols. Similar to the existing works presented in [11], the multi-path scattered environment is considered. The channels are block Rayleigh fading channels, i.e., the channel coefficient matrix $\boldsymbol{H}$ is constant during the transmission of one symbol, but is randomly changing between symbols. Different channels are identically distributed and statistically independent. Binary phase shift keying (BPSK) is chosen as the modulation scheme. 100 received symbols are used in the proposed algorithms for compromised nodes identification. The maximum likelihood detector is used for symbol demodulation.

Since compromised nodes detection is performed between one transmitting virtual MIMO node and one receiving virtual MIMO node, the performance evaluation only evaluates one hop to demonstrate the effectiveness of the proposed algorithm. For the simplicity, we assume that $|PreA| \leq |A|$. In the case that $|PreA| < |A|$, $PreA$ uses more than one rounds to detect the compromised nodes in A (see compromised nodes detection algorithm in Section 4.2), which doesn't affect the accuracy and performance of the proposed approach. Figure 6 shows the accuracy of the proposed algorithm for compromised nodes detection, where $PreA$ consists of four primary nodes and four primary nodes in A transmit simultaneously. Among the four nodes in A, three of them are compromised, which is the worst scenario. The accuracy is defined as the ratio of correctly identified compromised nodes and normal nodes to all nodes. It is clear that the proposed algorithm has close to 100% identification accuracy even when the signal-to-noise ratio (SNR) is as low as -4dB. It also shows that comparing with [21], the proposed scheme can detect significantly larger number of compromised nodes (three *vs.* one) with similar accuracy and the same number of primary nodes in detection cluster. In a cognitive radio network, the cooperative transmission nodes have to null out of the direction to the licensed primary user. The number of compromised nodes in A can be up to two when $|PreA| = 4$ according to Section 6. The accuracy is similar to that showed in Figure 6.

Figure 7 compares the performance of the proposed cooperative communication system with the conventional system that does not detect compromised nodes in terms of bit error rate (BER) of A. Considering the worst scenario, there are three compromised nodes and only one normal node in A. The detection cluster $PreA$ has 4 or 5 primary nodes. The results represented by lines are for 5 primary nodes case, while the results represented by lines with diamond symbols are for 4 primary nodes case. The BER performance of the system when there is no compromised nodes is also presented with the dashed line as a reference of the optimum performance. The dash-dot line is for the conventional system where the compromised nodes are not detected and uses the garbled data from the compromised nodes in symbol demodulation. The solid line is for the proposed system. Comparing with the conventional system, it is clear that the proposed system improves the reliability of the communication with only one normal node when SNR is higher than -8dB. Comparing with the system without compromised node, the performance loss of the proposed system is because there is no diversity gain with only one normal receiving node. This simulated case is the worst scenario.

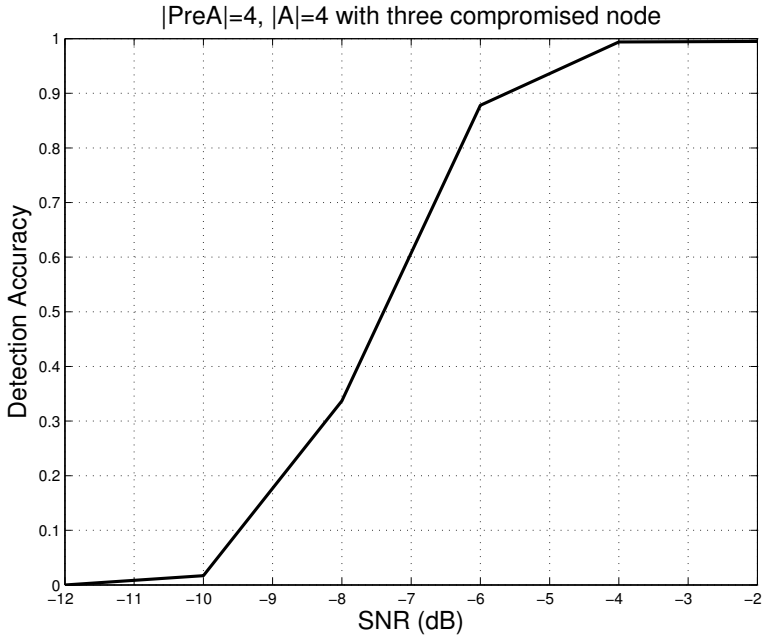

Figure 6: Accuracy of the proposed compromised nodes detector

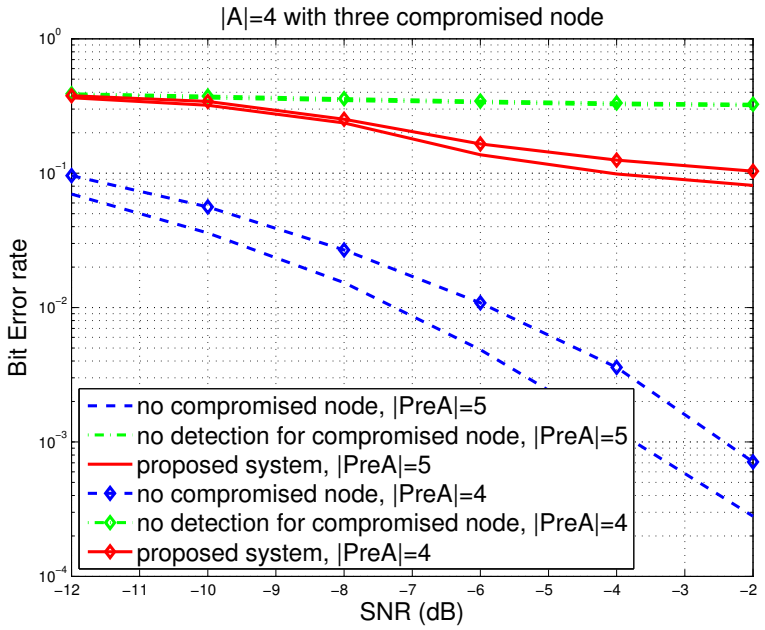

Figure 7: Performance comparison

The performance will be better when there are more than one normal receiving nodes. Figure 7 also shows that the performance is better for the proposed system with $|PreA| = 5$ than with $|PreA| = 4$ due to a bit higher diversity gain. On the other hand, the performance of the conventional system where the compromised nodes are not detected remains the same even with higher diversity gain. This is because the garbled data significantly reduces the data integrity.

Figure 7 presents the worst scenario under compromised nodes attack where there are three compromised nodes and only one normal node in transmitter cluster. Moreover, when SNR is -2

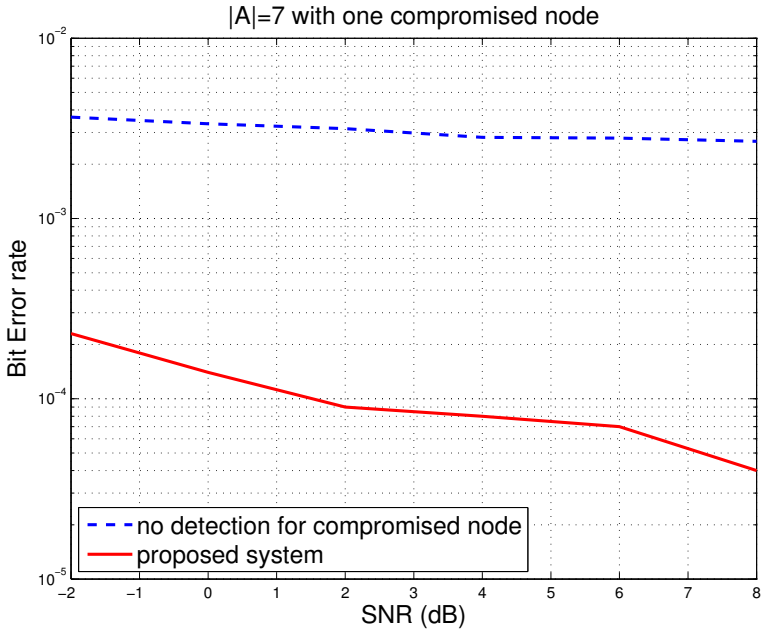

Figure 8: System performance with higher SNR and fewer compromised nodes

dB, the channel is still very noisy. Therefore, after excluding the compromised nodes in information relay, the performance of proposed system in terms of BER (≈ 0.1 at -2 dB SNR) may not be suitable for some WSN applications. When the SNR is higher, or there are fewer compromised nodes, or both, the BER will be much lower and the system performance (≈ 0.00004 at 8 dB SNR) will be suitable for most WSN applications as shown in Figure 8. In Figure 8, the SNR is from -2 dB to 8 dB and there is only one compromised node with six normal nodes in transmitter cluster.

Figure 9 and 10 demonstrate the capability of the distributed beamforming based information leaking prevention through radiation patterns. Figure 9 shows the radiation pattern in polar plot and 10 shows the radiation pattern in log plot. We assume the worst scenario that there are three compromised nodes in A located in 70, 90, and -20 degrees and only one normal node located in 30 degrees. After compromised node detection, four nodes in $PreA$ cooperatively form a beam toward the normal node and null out the compromised nodes' directions to prevent information leak. The obvious notches in the compromised nodes' directions and peak in normal node's direction guarantee that there is no degradation in normal node communication and no information leak to the compromised nodes. In a cognitive radio network, when $|PreA| = 4$ and $|A| = 4$, the number of compromised nodes in A can be up to two. In Figures 9 and 10, three compromised nodes can be considered as one primary user and two compromised nodes.

More simulations have been conducted for all the cases with $2 \leq |PreA| \leq 7$, $2 \leq m_T \leq 7$, and $-12 \leq SNR \leq 20$. Due to the page limits, these results are not presented here but available upon request. All the results lead to the same conclusion that the proposed schemes significantly improved capability to detect larger number of compromised nodes in A when comparing with [21].

8 Conclusion

Taking into query-based information collection applications, this paper proposed a cross-layered approach for security enhancement in cooperative MIMO communication system under active compromised nodes attack. To provide better communication security, the scheme combines cryptographic technique implemented in higher layers to overcome the external attacks and data assurance analysis at the physical layer to suppress the impact of the compromised relay nodes that try to corrupt the communications by sending garbled signals. The cryptography secures data transmission between

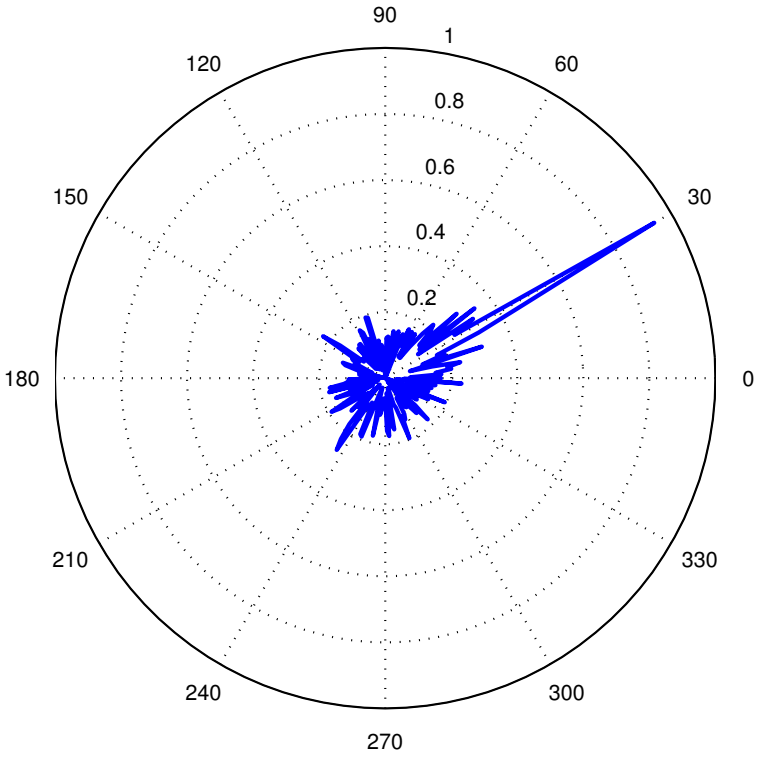

Figure 9: Polar plot of radiation pattern for normal node locates at 30^o, while compromised nodes locate at 70^o, 90^o, and -20^o

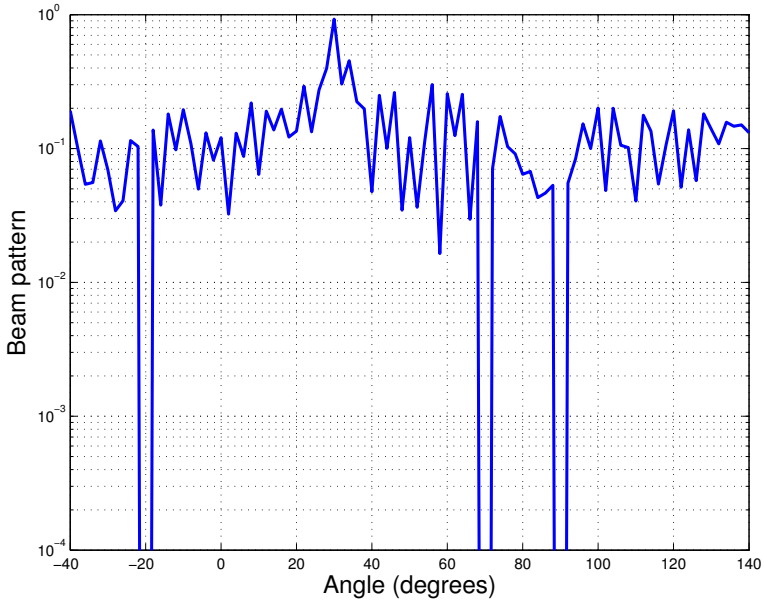

Figure 10: Log plot of radiation pattern for normal node locates at 30^o, while compromised nodes locate at 70^o, 90^o, and -20^o

authorized nodes and key revocation and network recovery. Comparing with our previous work, an upgraded information theory based algorithm for compromised nodes detection is proposed to

detect significantly larger number of possible compromised nodes. When the compromised nodes are detected through a round-trip process, distributed transmit beamforming is used to prevent information leaking before the completion of key revocation. The effectiveness and efficiency of the proposed algorithm for compromised nodes detection and information leaking prevention are demonstrated through computer simulations. The simulation results also show the significant improvement in the accuracy of received information. Furthermore, the proposed security scheme is modified and applied to cognitive radio networks by using the beamforming technique to avoid interference towards the licensed users.

Acknowledgment

This work was partially supported by U.S. Air Force Research Laboratory (AFRL) Research Collaboration Program (RCP) Contract FA8650-13-C-5800, National Science Foundation (NSF) Division of Graduate Education (DGE) Award 1438924, and NSF Division of Computer and Network Systems (CNS) Award 1405681.

References

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114, 2002.

[2] J. Mietzner, R. Schober, L. Lampe, W. H. Gerstacker, and P. A. Hoeher, "Multiple-antenna techniques for wireless communications - a comprehensive literature survey," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 2, pp. 87–105, 2009.

[3] S. Hussain, A. Azim, and J. H. Park, "Energy efficient virtual MIMO communication for wireless sensor networks," *Telecommun. Syst.*, vol. 42, no. 1, pp. 139–140, 2009.

[4] S. Jayaweera, "Virtual MIMO-based cooperative communication for energy-constrained wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 5, no. 5, pp. 984–989, 2006.

[5] W. Chen, Y. Yuan, C. Xu, K. Liu, and Z. Yang, "Virtual MIMO protocol based on clustering for wireless sensor network," in *Proc. IEEE Symp. Computer and Communications*, pp. 335–340, 2005.

[6] J. Liu, "Energy-efficient cross-layer design of cooperative MIMO multi-hop wireless sensor networks using column generation," *Wireless Personal Communications Journal*, vol. 66, no. 1, pp. 185–205, 2012.

[7] M. R. Islam and J. Kim, "Energy efficient cooperative MIMO in wireless sensor network," in *Proc. IEEE International Conference on Intelligient Sensors, Sensor Networks and InformationProcessing (ISSNIP*, pp. 505–510, 2008.

[8] W. Chen, H. Miao, and L. Hong, "Cross-layer design for cooperative wireless sensor networks with multiple optimizations," *International Journal of Networking and Computing*, vol. 1, no. 1, pp. 63–81, 2011.

[9] Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks, a survey," *IEEE Commun. Surveys Tuts.*, vol. 10, no. 3, pp. 6–28, 2008.

[10] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," in *Proc. 1st IEEE International Workshop on Sensor Network Protocols and Applications*, pp. 113–127, 2003.

[11] Y. Mao and M. Wu, "Tracing malicious relays in cooperative wireless communications," *IEEE Trans. Inform. Forensics Security*, vol. 2, no. 2, pp. 198–212, 2007.

[12] X. Chen, K. Makiki, K. Yen, and N. Pissinou, "Sensor network security: a survey," *IEEE Commun. Surveys Tuts.*, vol. 2, no. 2, pp. 198–212, 2007.

[13] A. Jain, K. Kant, and M. R. Tripathy, "Security solutions for wireless sensor networks," in *Proc. IEEE Second Intl. Conf. Advanced Computing & Communication Technologies*, pp. 430–433, 2012.

[14] V. C. Sekhar and M. Sarvabhatla, "Security in wireless sensor networks with public key techniques," in *Proc. IEEE Intl. Conf. Computer Communication and Informatics*, pp. 1–16, 2012.

[15] H. K. D. Sarma, A. Kar, and R. Mall, "Secure routing protocol for mobile wireless sensor network," in *Proc. IEEE Sensors Applications Symposium*, pp. 93–99, 2011.

[16] X. Li and J. Hwu, "Using antenna array redundancy and channel diversity for secure wireless transmissions," *Journal of Communications*, vol. 2, no. 3, pp. 24–32, 2007.

[17] H. Kim and J. D. Villasenor, "Secure MIMO communications in a system with equal numbers of transmit and receive antennas," *IEEE Commun. Lett.*, vol. 12, no. 5, pp. 386–388, 2008.

[18] H. Wen and G. Gong, "A MIMO based cross-layer approach to augment the security of wireless networks," *Technical Report CACR 2008-21, University of Waterloo*, 2008.

[19] W. Chen, M. McNeal, and L. Hong, "Cross-layered design of security scheme for cooperative MIMO sensor networks," in *Proc. IEEE Intl. Conf. Wireless Information Technology and Systems (ICWIT)*, pp. 1–4, 2010.

[20] L. Hong, M. McNeal, and W. Chen, "Secure cooperative MIMO communications under active compromised nodes," in *Proc. IEEE Intl. Workshop on Sensor Networks and Systems for Pervasive Computing (PerSeNS)*, pp. 128–133, 2011.

[21] L. Hong and W. Chen, "Information theory and cryptography based security scheme for cooperative MIMO networks," *ELSEVIER, Ad Hoc Networks*, vol. 14, pp. 95–105, 2014.

[22] W. Chen, L. Hong, S. Shetty, D. Lo, and R. Cooper, "Cross-layered security approach with compromised nodes detection in cooperative sensor networks," in *Proc. IEEE Workshop on Advances in Parallel and Distributed Computational Models*, 2016.

[23] J. N. Leneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inform. Theory*, vol. 50, no. 12, pp. 3062–3080, 2004.

[24] J. G. Proakis, *Digital Communications*, vol. 5. 2008.

[25] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 8, pp. 1451–1458, 1998.

[26] S. Senthikumar and C. G. Priya, "A review of channel estimation and security techniques for CRNS," *Automatic Control and Computer Sciences*, vol. 50, no. 3, pp. 187–210, 2016.

[27] R. Mudumbai, D. R. B. III, U. Madhow, and H. V. Poor, "Distributed transmit beamforming: Challenges and recent progress," *IEEE Comm. Magazine*, vol. 47, no. 2, pp. 102–110, 2009.

[28] S. Cui, A. J. Goldsmith, and A. Bahai, "Energy-efficiency of MIMO and cooperative MIMO techniques in sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 22, no. 6, pp. 1089–1098, 2004.

[29] X. Du, M. Guizani, Y. Xiao, and H.-H. Chen, "A routing-driven elliptic curve cryptography based key management scheme for heterogeneous sensor networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1223–1229, 2009.