On Security and Reliability using Cooperative Transmissions in Sensor Networks

Aylin Aksu, Prashant Krishnamurthy, David Tipper
School of Information Sciences
University of Pittsburgh
Pittsburgh, PA 15260
Email: {aaksu, prashant, tipper}@tele.pitt.edu

Ozgur Ercetin
Faculty of Engineering and Natural Sciences
Sabanci University
Istanbul, Turkey
Email: oercetin@sabanciuniv.edu

***Abstract*—Recent work on cooperative communications has demonstrated benefits in terms of improving the reliability of links through diversity and/or increasing the reach of a link compared to a single transmitter transmitting to a single receiver (single-input single-output or SISO). In one form of cooperative transmissions, multiple nodes can act as virtual antenna elements and provide such benefits using space-time coding. In a multi-hop sensor network, a source node can make use of its neighbors as relays with itself to reach an intermediate node, which will use its neighbors and so on to reach the destination. For the same reliability of a link as SISO, the number of hops between a source and destination may be reduced using cooperative transmissions. However, the presence of malicious or compromised nodes in the network impacts the use of cooperative transmissions. Using more relays can increase the reach of a link, but if one or more relays are malicious, the transmission may fail. In this paper, we analyze this problem to understand the conditions under which cooperative transmissions may fare better or worse than SISO transmissions.**

I. Introduction

Cooperative diversity is a relatively new physical layer approach which helps to achieve performance gains similar to multiple-input multi-output (MIMO) enabled transmissions in wireless networks compared to traditional single-input single-output (SISO) links. With cooperative transmissions, several nodes with single antennas form a *virtual antenna array* to assist each other with the transmission of messages. When a virtual antenna array is created only for transmitting to a single receiving node, the approach is called virtual multiple-input single-output (vMISO) [1]. The way vMISO works is as follows. A cooperative transmission is initiated by a source node multi-casting (or broadcasting) a message to a number of cooperating relay nodes, which then send the message to the destination node (together with the source node) using techniques such as space-time coding. The destination node combines the signals from the source and relays appropriately to decode the message. Cooperative transmissions exploit a fundamental feature of the wireless medium: the ability to achieve *diversity* through independent channels created between the multiple transmitters and the receiver, because these channels are likely to fade independently. The resulting advantages (widely studied previously at the physical layer [2]) are a better bit-error rate (BER) for a given transmission rate and/or a longer transmission range for a given BER while consuming the same amount of transmission power compared to non-cooperative transmissions. These advantages can also provide energy efficient routing and a longer lifetime for sensor networks. From a security point of view, cooperative transmissions suffer from drawbacks. With more relay nodes, a higher order of diversity can be achieved improving the BER and/or range with cooperative transmissions. However, at the same time, security threats increase with the involvement of additional parties to the communication. For example, even if one of the nodes that form the virtual antenna array is malicious, it can disrupt the transmission, or it can transmit garbled symbols in order to both corrupt the transmission and drain the batteries of honest nodes.

In this paper, we develop a framework for evaluating the performance difference between using cooperative transmissions or not for successful reception of packets in sensor networks with a mix of honest and malicious and/or compromised nodes. While this could apply for any multi-hop wireless network, we consider here a sensor network with multi-hop transmissions where key pre-distribution schemes may be employed for security [3]. Even with key pre-distribution, *not all pairs* of sensor nodes share a key, but many pairs do. Thus, it is very likely that each SISO link on a route from a source to the destination is secure when there are no compromised nodes. The presence of compromised nodes will however disrupt a path from the source to the destination and data packets will not successfully reach the destination. As the number of hops to the destination increases, the chance of a successful reception at the destination drops. When cooperative transmissions are employed with vMISO, for the same link reliability, the number of hops to the destination may be reduced making it more likely that the packet is successfully received at the destination (see Figure 1). The reduction in the number of hops increases as the number of cooperating nodes increases. However, not all of the potential cooperating nodes may share a key and/or some of these nodes may be compromised or malicious. In such cases, vMISO may fare worse than longer SISO links.

It is not easy to predict what circumstances are better for vMISO or SISO for various reasons. First, the diversity benefits increase with the number of cooperating relays, but the relation is non-linear. Second, the chance of involvement

of malicious or compromised nodes depend on their number in the network and the distance between source and destination. Third, various key pre-distribution schemes have different probabilities of sharing secret keys with neighbors that may act as relays. The contribution of this paper is an analytical framework that includes these parameters so that it is possible to evaluate the boundaries of where vMISO or SISO fare better. We do however make simplifying assumptions (e.g., we do not explicitly account for node density). Our analysis allowed us to determine a general condition where vMISO has a better probability of successfully delivering a packet than SISO as $nK_v < K_s$, where n is the number of cooperating nodes that is used at each hop of a multi-hop vMISO route, and K_v and K_s are the number of hops required to reach a destination from the source with vMISO and SISO, respectively. This condition holds when the number of honest nodes in the neighborhood of a node is much higher than n. As expected, our analysis shows that while using vMISO, a small n is preferable.

The rest of the paper is organized as follows. In section II, we present some background and related work on cooperative transmissions and some possible attacks against cooperative transmissions. Section III describes the framework for analyzing the probability of successfully receiving a packet at the destination with SISO and vMISO, with and without the use of shared keys. Section IV presents the results obtained from the analysis. Section V concludes the paper and outlines its limitations.

II. Background and Related Work

In this section we briefly describe the background material needed for the rest of this paper and some related work. We do not look at an exhaustive review of the literature on cooperative diversity for which we refer to [1], [2], [4].

A. Cooperative Transmissions

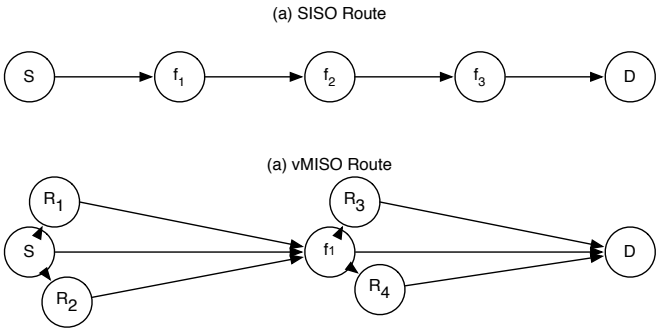

Fig. 1. Example of a SISO route and a vMISO route between a source and destination node

Cooperative transmissions can improve the quality or range of a link by creating virtual antenna arrays comprised of a source and some of its neighbors. In a vMISO system, a cluster of cooperating nodes emulate the antenna array of a real MISO system [1]. There is a single *head node* in this cluster that is the originator of data, and there are multiple *cooperating nodes* each of which act as a transmitter antenna in an antenna array. Unlike real MISO systems, antennas are not co-located in vMISO systems. The source first broadcasts or multicasts its packet to its neighboring relays and they all then simultaneously transmit the packet to the receiver(s). Once all nodes in the cluster have the original data, they can encode data using an appropriate *space-time block code* (STBC) [5], and simultaneously transmit the coded block to a receiver. Figure 1 shows examples of SISO and vMISO routes between a source S and a destination D. The SISO route is 4 hops long and goes through intermediate nodes f_1, f_2, f_3. The vMISO route is two hops long, but each hop has three transmitters (S, R_1, R_2 for the first hop and f_1, R_3, R_4 along the second hop). The assumptions underlying the benefits from vMISO are that each *individual link* (e.g., S to f_1 or R_2 to f_1) in Figure 1 is independently fading. Thus, the vMISO link is more reliable because of the inherent diversity.

There are several physical layer related issues that we do not elaborate upon here. It is possible to overcome these challenges using physical layer techniques [1]. For example, in order to leverage the benefits of space-diversity, data should be encoded by a space time block code. An STBC with code rate $r_n = k/k_n$, $r_n \leq 1$, is defined by a transmission matrix of size $k_n \times n$, where n is the number of (virtual) transmitter antenna elements and k_n is the number of time units involved in the transmission of k symbols [5]. The simplest STBC is the Alamouti code, which has unit rate [6], $n = 2$ co-located antennas or $n = 2$ cooperating relays, and transmitting two symbols every two time units. STBCs suitable for higher numbers of transmitter antennas or cooperating relays have also been developed (see for e.g., [7]). In order to decode the transmitted block successfully, the receiver node requires channel state information (CSI) between itself and each of the transmitting nodes. CSI is obtained by using pilot tones transmitted by each node prior to the data transmission. Some loose synchronization between S, R_1 and R_2 is necessary but the impact of different node locations (as against colocated antennas) has been shown to be minimal [1]. The *individual links* are typically assumed to be flat-fading.

In this paper, we ignore the protocols and overhead associated with identifying nodes such as R_1 and R_2 at every link as this has been previously considered in other work and is also not the focus of this paper. For instance, in [1] a primary SISO route is first created and then this primary route is used to create a vMISO route. In [2], a greedy geographical routing scheme is used. We also ignore the medium access issues in this paper. Modifications to the traditional request-to-send (RTS) and clear-to-send (CTS) handshakes to avoid collisions and hidden terminals are possible [1].

B. Security Threats Against vMISO

Wireless ad hoc and sensor networks are vulnerable to security attacks due to the shared nature of wireless medium and the way they are deployed and their limited resources. Cooperative transmissions are more vulnerable to some security attacks than non-cooperative (SISO) transmissions, because

they aim to exploit the advantages of diversity achievable with multiple transmitters. In this section, we will give a brief explanation of potential attacks. Our focus later in the paper is less on the attacks and more on the impact. Irrespective of the cause of the attack, we assume that the goal of a malicious or a compromised node is to disrupt the successful reception of packets. Other attacks mentioned here (e.g., eavesdropping or wormhole attacks) are outside the scope of this paper.

1) Disruption of Packet Transmission on vMISO Links: vMISO transmissions can exploit space-time diversity by using relay nodes. A relay node must agree to help a source node which has a data to send to a destination node. When a relay node *behaves selfishly* by not cooperating, a source node cannot exploit the advantages of cooperative transmissions, and instead it has to use SISO transmissions or transmissions with fewer cooperating nodes. This may result in conditions such as higher power consumption, longer latency in transferring data and/or higher bit error rates. A selfish node that agrees to cooperate but then does not transmit the packet with the source and other relays reduces the diversity and will likely result in a packet not reaching the destination reliably.

The number of relays is very important in cooperative transmissions. Therefore, an attacker may try to prevent a source node from choosing the right number of relays for the cooperative transmission. Sybil attacks can be an example for this kind of an attack. For example, a Sybil node can claim more than one identity, which will cause the source node to believe that it has n relays, while in reality it has $m < n$ relays. If STBC is used as part of the cooperation scheme, the cooperative transmission simply is not realized. If any other uncoded cooperation scheme is used, given certain BER requirements, a source node cannot transmit its data to the destination which is in the transmission range if there are n nodes in the cooperation set, but outside the range if there are $m < n$ nodes. The necessity of symmetric links in cooperative transmissions adds another problem to the mix. For a symmetric cooperative link between source and destination nodes, they both must have at least the same number of relays. For example, if a source node has n relays, the destination must also have at least n relays.

With a routing algorithm where the routing metric favors nodes with higher numbers of relays, a malicious node may try to convince others that it has a higher number of relays in its neighborhood or that other nodes have fewer relays. This way it may attract traffic to itself which then never reaches the destination.

An attacker can jam the channel during the transmission of pilot tones that are often needed with cooperative transmissions in order to prevent successful estimation of CSI at the receiver. In such a case, the receiver cannot decode symbols successfully. Selectively jamming some transmissions will also damage packets at the receiver. In addition, control packet corruption attacks are possible that allow a malicious node to disrupt the successful reception of a packet.

2) Other Attacks: One of the advantages of cooperative diversity is the increased transmission range with the same BER requirement and power consumption as SISO transmissions. However, this causes a single hop cooperative transmission to have wider reception and interference ranges when compared to those of SISO transmissions. Therefore, cooperation has increased vulnerabilities in terms of overhearing due to the larger transmission range. This can facilitate *Rushing and Wormhole Attacks*. A wormhole attack may occur when a malicious node captures a packet and replays it at another location. A rushing attack may occur when a malicious node does not wait for timers to timeout and replies before a legitimate node. Obviously, the chances that a malicious node can overhear a cooperative transmission is higher. In addition, cooperative transmissions often require a more complex MAC algorithm [1] which requires exchanging more messages than needed for a direct transmission. This also increases the probability of attacks that are related to packet capturing. Methods that narrow down the transmission area without decreasing transmission range in the desired direction, i.e., using directional antennas, may be useful.

Cooperative jamming introduces noise into the communication medium to hurt the eavesdropper (untrusted relay) more than the legitimate destination. An example of such a solution to mitigate the eavesdroppers in the transmission range is given in [8], where an opportunistic selection of two relay nodes is proposed to increase security against eavesdroppers. The first relay operates as a conventional node and assists a source to deliver its data to a destination via the Decode-and-Forward strategy [9]. The second relay is used in order to create intentional interference at the eavesdropper nodes. The proposed selection technique jointly protects the primary destination against interference and jams the reception at the eavesdropper. This assumes knowledge of the existence of the eavesdropper. In [10], the authors show that a positive secrecy rate can be achieved with the help of destination node or an external node that jams the relay by cooperative jamming.

Resource draining attacks aim to reduce or deplete the network's resources such as the battery power of nodes and the capacity of the network, etc. A malicious node that is involved in a cooperative transmission can attack the transmission to drain the batteries of honest nodes, or occupy links by sending garbage data for a longer time to decrease the capacity of the network. Relay discovery attacks may result in high numbers of retransmissions which will drain the batteries of nodes and reduce the lifetime of the network. As mentioned before, the nodes that reside in the wide transmission range of a cooperation set (set of nodes cooperating) have to wait to be able to send their own data. In a non-cooperative transmission, a simple 4-way handshake is often enough to contend for the channel; in the vMISO case, however, transmission latency increases due to the message exchanging phase at the source and destination clusters before cooperative control packets are sent; also coding and decoding of symbols at the source and destination add to the latency. Therefore, retransmissions must be as few as possible to have a longer network lifetime.

In [11], two types of resource draining attacks are addressed. In "inside" attacks, malicious nodes send garbage information

to the destination when they serve as relays. In bad mouthing attacks, a malicious node needs to report the link quality or trust values. The malicious node can lie and report false information. To mitigate both attacks in addition to selfish behavior, [11] proposed a distributed trust-assisted cooperative transmission scheme. Trust values are constructed to determine the link quality between cooperating nodes and the destination node. Relayed transmissions are combined at the destination according to the trust values.

Injecting traffic attacks are addressed in [12]. These attacks occur when attackers inject an overwhelming amount of traffic into the network to consume good nodes' valuable network resources and reduce the network's lifetime. In cooperative mobile ad hoc networks, nodes will usually unconditionally forward packets for other nodes. Consequently, such networks are extremely vulnerable to injecting traffic attacks, especially those launched by inside attackers. In [12], two types of injecting traffic attacks that can be launched in cooperative ad hoc networks are mentioned: query flooding attack and injecting data packet attack (IDPA). Fortunately, in cooperative ad hoc networks, since nodes belong to the same authority and pursue common goals, it is possible that they can know each other's data packet injection statistics. According to the solution proposed in [12], detecting injecting traffic attacks is equivalent to detecting those nodes who are not legitimate, yet they inject packets into the network or whose packet injection rates are much higher than their legitimate upper bounds. Also, legitimate nodes add a header to their packets along with a signature. The maximum number of allowed hops and signatures in the headers are used by honest nodes in order to decide if there exists a malicious node on the route and whether to forward a packet to the next hop or not.

C. Key Pre-distribution in Sensor Networks

One of the problems in the security of sensor networks is that the nodes cannot store a lot of keys and it is not wise to use a single key that every node shares as a single node compromise can disrupt the whole network. To address this problem, in [13], a key management mechanism is proposed, and it has 3 phases: key pre-distribution, shared-key discovery, and path-key establishment. The key-predistribution phase is an offline phase, where a large pool of S keys are generated. A key ring is generated from k keys that are randomly chosen from this pool. Key identifiers for each key in the key ring are loaded to a sensor node. In the shared-key discovery phase, each node discovers its neighbors in communication range with which it shares key(s). Nodes discover shared-keys by broadcasting the list of key identifiers of the keys on their key ring in clear text. After this phase, a secure link exists between two nodes if they share at least one key. In path key establishment phase, a path-key is assigned to selected pairs of nodes in wireless communication range that do not share a key but are connected by two or more links at the end of the shared-key discovery phase. The downside of this *random key distribution* scheme is that the probability that two nodes share a key can be small.

The knowledge of the deployment of sensors [14] may be used to improve this probability to something close to 1. Multiple key pools are used in this *deployment based scheme* as opposed to the single global key pool S. Sensors are assumed to be deployed in clusters or groups organized into a grid. Each deployment group has its own associated group key pool that is generated from the global key pool. Keys from the global key pool are assigned to group key pools in a way that the group key pools of clusters that are geographically closer have a certain number of *common* keys. However, if two clusters are not neighbors, the group key pools do not share any keys. Nodes that are very far apart are thus unlikely to share any keys.

In this paper, we make use of these key pre-distribution approaches to increase the reliability of SISO and vMISO transmissions in the presence of malicious and/or compromised nodes as explained in the following sections.

III. Framework for Analyzing Packet Success with vMISO and SISO Transmissions

In this section, we describe an analytical framework for evaluating the probability of successfully delivering a packet with SISO and vMISO transmissions in the presence of malicious nodes in the system.

A. Outage Probability and Transmission Range

Based on [2], we first derive here an expression for the relationship between the outage probability, the number of cooperating nodes, and the increase in transmission range possible with vMISO. We assume a narrow-band multi-path wireless channel with a coherence time longer than the symbol transmission time. This channel is modeled as a flat Rayleigh fading channel with a path-loss exponent β. All nodes have omni-directional antennas and emit signals at the same power P_t. The large scale path loss for a transmitter-receiver distance of d is, $Kd^{-\beta}$, where K is a constant that is typically a function of λ, the wavelength. For a certain packet transmission, each transmitted signal goes over an independent Rayleigh fading channel and it is corrupted by a zero-mean additive white Gaussian noise (AWGN). Let α be a Rayleigh distributed random variable with parameter $\sigma = 1$. We note here that $|\alpha|^2$ has an exponential distribution. Under Rayleigh fading with SISO, the signal strength $S_s = P_0 d_s^{-\beta}|\alpha|^2$ at the receiver is exponentially distributed, where $P_0 = P_t \times K$. Here d_s is the distance between the SISO transmitter and receiver.

Let α_i for $i = 1, 2, \cdots, n$ be independent random fading coefficients with Rayleigh-distributed magnitude and uniform phase. If there are n cooperating transmitters $i = 1, 2, \cdots, n$ in vMISO at distances d_i from the receiver, the signal strength S_i of the i-th cooperating node's signal at the receiver will be $P_0|\alpha_i|^2 d_i^{-\beta}$ and the overall signal strength will be $S = P_0 \sum_{i=1}^{n} |\alpha_i|^2 d_i^{-\beta}$. If we make the assumption that the d_i's are very close and equal to d_v, the signal strength at the receiver is $S_v = P_0 d_v^{-\beta} \sum_{i=1}^{n} |\alpha_i|^2$. Note that $\sum_{i=1}^{n} |\alpha_i|^2$ has a χ^2 distribution with $2n$ degrees of freedom.

The quality of the wireless link can be measured by the instantaneous bit error rate (BER). It is well-known that spatial diversity can help transmit with a lower total energy per symbol, while satisfying the same BER requirement [15]. However, the analysis involving BER must assume a certain modulation class and involves complicated mathematical functions. A more general way to capture the link quality is through the outage probability, p_{out}, defined as the probability that the instantaneous signal-to-noise-ratio (SNR), SNR_i, falls below a certain threshold. If the coherence time is greater than the packet transmission time, the outage probability is time-invariant for a given packet transmission. Suppose that S_{th} is the minimum required signal strength for correct decoding at the receiver for a target outage probability p_{out} (assuming that the AWGN does not change with time). Then, the outage probability for the random signal strength S at the receiver can be calculated as,

$$p_{out} = Pr\left[S \leq S_{th}\right] \tag{1}$$

For the same p_{out}, SISO and vMISO will have different transmission ranges as follows.

$$\begin{aligned} p_{out} &= Pr\left[S_s \leq S_{th}\right] = Pr\left[P_0 d_s^{-\beta}|\alpha|^2 \leq S_{th}\right] \\ &= Pr\left[|\alpha|^2 \leq \frac{S_{th} d_s^{\beta}}{P_0}\right] \qquad (2) \\ \Rightarrow\ d_s^{\beta} &= F_s^{-1}(p_{out})\frac{P_0}{S_{th}} \qquad (3) \end{aligned}$$

$$\begin{aligned} p_{out} &= Pr\left[S_v \leq S_{th}\right] = Pr\left[P_0 d_v^{-\beta}\sum_{i=1}^{n}|\alpha_i|^2 \leq S_{th}\right] \\ &= Pr\left[\sum_{i=1}^{n}|\alpha_i|^2 \leq \frac{S_{th} d_v^{\beta}}{P_0}\right] \qquad (4) \\ \Rightarrow\ d_v^{\beta} &= F_v^{-1}(p_{out})\frac{P_0}{S_{th}} \qquad (5) \end{aligned}$$

where $F_s(\cdot)$ and $F_v(\cdot)$ are respectively the cumulative exponential and χ^2 ($2n$ degrees of freedom) distributions previously mentioned. Thus, the gain in range for the same outage probability [2] can be expressed as:

$$\frac{d_v}{d_s} = \left[\frac{F_v^{-1}(p_{out})}{F_s^{-1}(p_{out})}\right]^{\frac{1}{\beta}} = G_n(p_{out}, \beta) \tag{6}$$

We note here that the number of cooperating nodes n appears as an argument through the degrees of freedom of the χ^2 distribution.

B. Probability of Success without Malicious Nodes

First, let us suppose that a source node wishes to send a packet to a destination node at distance D using only SISO transmissions. Let the *minimum* number of hops given an outage probability p_{out} be $K_s = \left\lceil \frac{D}{d_s} \right\rceil$. If there are no malicious nodes in the network, the probability that a packet is successfully received at the destination is equal to the probability that the packet is successfully received on every hop,

$$P_{suc}^{SISO} = (1 - p_{out})^{K_s} \tag{7}$$

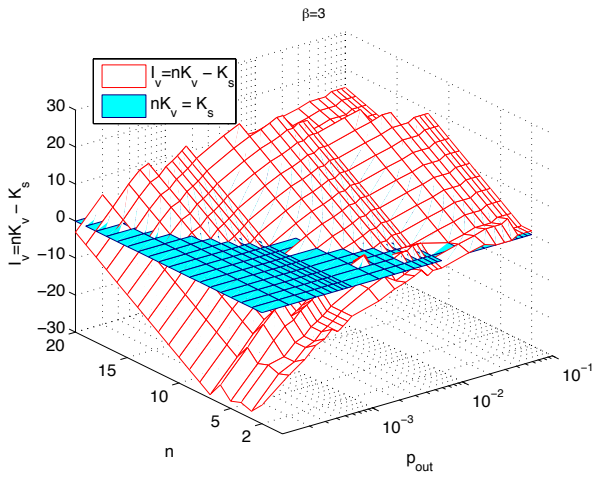

Fig. 2. $I_v(n, p_{out}, \beta) = nK_v - K_s$

When vMISO transmissions with n cooperating nodes at each hop are employed, the minimum number of hops needed from the same source to the same destination becomes $K_v = \left\lceil \frac{D}{d_v} \right\rceil = \left\lceil \frac{K_s}{G_n(p_{out},\beta)} \right\rceil \leq K_s$. To calculate the success probability with vMISO, we need to consider the SISO transmissions between source and relay nodes in addition to the cooperative transmission to the destination node in every hop of the multi-hop vMISO route. Then, the success probability will be,

$$P_{suc}^{vMISO} = (1 - p_{out})^{nK_v} \tag{8}$$

Theorem 1 (vMISO reliability without malicious nodes): With no malicious nodes in the network and n cooperating nodes to transmit a data from a source to a destination that is K_s SISO hops away, vMISO has better transmission reliability than SISO if $I_v(n, p_{out}, \beta) = n\left\lceil \frac{K_s}{G_n(p_{out},\beta)} \right\rceil - K_s < 0$, given an outage probability p_{out} and path-loss exponent β.

Proof: When we compare (7) and (8), vMISO performs better than SISO when,

$$\begin{aligned} P_{suc}^{vMISO} &> P_{suc}^{SISO} \\ (1 - p_{out})^{nK_v} &> (1 - p_{out})^{K_s} \\ nK_v &< K_s \\ I_v(n, p_{out}, \beta) = n\left\lceil \frac{K_s}{G_n(p_{out},\beta)} \right\rceil - K_s &< 0 \qquad (9) \end{aligned}$$

■

Theorem 1 says that the performance of vMISO compared to SISO depends on β, n and p_{out}. It is not possible to simplify this further easily due to the ceiling function used to calculate the number of hops. We plot $I_v = nK_v - K_s$ in Figure 2 to show n and p_{out} values for which vMISO is more reliable than SISO, $I_v < 0$ (from Theorem 1), when $\beta = 3$. From this figure, we observe that for vMISO to perform better, p_{out} and n must be small, or as p_{out} gets larger, n must be smaller. When $\beta = 4$, the ranges for n and p_{out} for which vMISO is better is narrower than for $\beta = 3$.

C. Probability of Success with Malicious Nodes

Next we consider the setup of routes between sources and destinations in the network and the impact that malicious nodes may have on the probability of successfully receiving a packet at the destination. We assume that source and destination nodes are honest nodes and any malicious node will participate in generating the route with the idea of dropping or corrupting data packets later. Let γ be the fraction of honest nodes in the network. Without any means of verifying whether or not a node in the network is malicious, the probability of picking a malicious node on a route depends on $1-\gamma$. We further let δ_s be the degree of a node (the number of neighbors) in SISO range d_s. Then, δ_s consists of both honest nodes and malicious nodes

$$\delta_s = \delta_h + \delta_m.$$

When there is no mechanism to verify a node's trustworthiness, an honest node cannot differentiate between honest and malicious neighbors; therefore, the fraction of honest nodes is $\gamma = \frac{\delta_h}{\delta_s}$. For a forwarding node to be on a "successful" route from a source to a destination (i.e., packets are not lost due to malicious activity), it should have at least 2 honest nodes in its SISO range (the previous and the next node on route). The probability that a source node chooses an honest forwarding node f_1 as the next hop node (from Figure 1) is γ, and the probability that f_1 chooses another honest node f_2 (excluding the source node) will be $1-\frac{\delta_m}{\delta_s-1}$. When $\delta_s >> 1$, this probability approaches $\gamma = \frac{\delta_h}{\delta_s}$. Similarly, if the density of nodes is high, and the fraction $1-\gamma$ of malicious nodes is also high, for simplicity, we can assume that this fraction does not change when a few nodes are already picked to be on a route. Essentially then, the probability of picking a malicious node as an intermediate node is $1-\gamma$.

On a SISO route of length K_s hops, none of the K_s-1 intermediate nodes (e.g., f_1, f_2, f_3 in Figure 1) must be malicious for the packet to be received successfully at the destination. Thus we have,

$$P_{suc}^{SISO} = (1-p_{out})^{K_s} \times \gamma^{K_s-1} \tag{10}$$

When vMISO transmissions with n cooperating nodes are employed, the computation of success probability is more complex. This is because, in this case, each forwarding node in vMISO range must be chosen from the honest neighboring nodes, and in addition, each cooperating relay in SISO range must be chosen from the honest nodes. Let P_n be the probability that an honest source node chooses $n-1$ honest relay nodes in its SISO range to cooperate with them in a single hop vMISO. Then,

$$P_n = \frac{\binom{\delta_h}{n-1}}{\binom{\delta_s}{n-1}} = \gamma \times \prod_{i=1}^{i=n-2} \frac{\delta_h - i}{\delta_s - i}. \tag{11}$$

We note that P_n increases with increasing δ_h (and correspondingly δ_s) although γ is constant. The reason is that the probability of selecting $n-1$ cooperating relays in a larger range is higher than in a smaller range. We analyze P_n for different ranges of n and δ_h while keeping $\gamma = \delta_h/\delta_s$ constant. There are three cases we consider:

1) When $\delta_h \to \infty$ and $\delta_h >> n$, $P_n \to \gamma^{(n-1)}$.
2) When $n = 2$, $P_n \to \gamma$.
3) When $n \to \infty$, $P_n \to 0$.

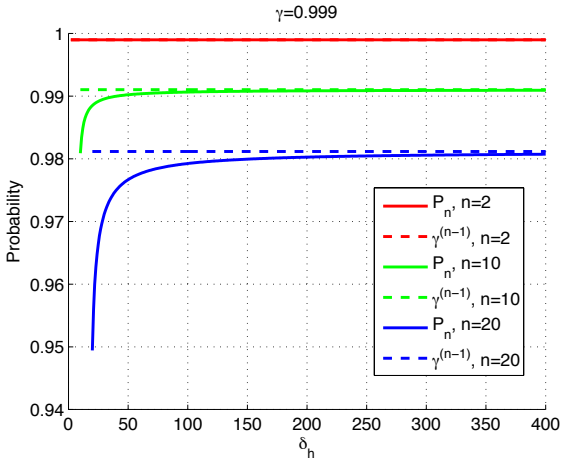

Fig. 3. P_n approximation

In Figure 3, we show P_n and $\gamma^{(n-1)}$, its approximation, for simplifying the analysis for various n. The observations from this figure validates that the approximation is very close to the exact value of P_n. For small n, $n < 10$ the difference is less than 0.01, and as n increases the error also increases. However, even for $n = 20$, the error is less than 0.03.

In a multi-hop vMISO route of length K_v hops, there exist K_v vMISO transmissions, and $K_v - 1$ forwarding nodes. Then, the success probability is given as,

$$P_{suc}^{vMISO} = (1-p_{out})^{nK_v} \times (P_n)^{K_v} \times \gamma^{(K_v-1)} \tag{12}$$

Theorem 2 (vMISO reliability with malicious nodes): When there exist malicious nodes in the network, but no mechanism exists to distinguish between them, using vMISO with n cooperating nodes to transmit a data from a source to destination at distance K_s SISO hops has better transmission reliability if $I_v(n, p_{out}, \beta) = n\left\lceil \frac{K_s}{G_n(p_{out},\beta)} \right\rceil < K_s$ given the same outage probability requirement, p_{out} and path loss exponent, β.

Proof: To simplify the analysis, we can compare P_{suc}^{vMISO} and P_{suc}^{SISO} ((12) and (10)) under three different cases:

1) **First case:** $\gamma << 1 - p_{out}$: This condition is similar to the case when there are no malicious nodes in the network, since the terms including γ in (10) and (12) can be neglected. P_n in (12) can also be neglected since it is also a function of γ. Then, this condition is in line with Theorem 1.
2) **Second case:** $1 - p_{out} = \gamma$ **and** $P_n \approx \gamma^{(n-1)}$: This condition is possible when $\delta_h \to \infty$ and $\delta_h >> n$ which results in $P_n \approx \gamma^{(n-1)}$. Then (10) and (12) can be re-

written as,

$$P_{suc}^{SISO} = \gamma^{2K_s-1} \quad (13)$$

$$P_{suc}^{vMISO} = \gamma^{(2nK_v-1)} \quad (14)$$

Then, comparing (13) and (14), vMISO performs better than SISO when $I_v = nK_v - K_s < 0$.

3) **Third case:** $\gamma >> 1 - p_{out}$ **and** $P_n \approx \gamma^{(n-1)}$: Under this condition, the $(1-p_{out})$ terms in (10) and (12) can be neglected, and they can be re-written as,

$$P_{suc}^{SISO} = \gamma^{K_s-1} \quad (15)$$

$$P_{suc}^{vMISO} = \gamma^{(nK_v-1)} \quad (16)$$

When we compare (15) and (16), vMISO performs better than SISO if $I_v = nK_v - K_s < 0$.

Note that in the presence of malicious nodes in the network and without a mechanism (e.g., shared keys) to identify malicious nodes, **all three cases result in the same condition** $I_v = nK_v - K_s < 0$ for a K_v hops vMISO route to outperform a K_s hops SISO route in terms of successful packet reception probability for given β and p_{out}. ■

From Theorems 1 and 2, we observe that the condition for multi-hop vMISO to outperform multi-hop SISO in terms of success probability in the presence of malicious nodes and with no mechanism for distinguishing between honest and malicious nodes is the same as the condition for multi-hop vMISO to outperform multi-hop SISO when there are no malicious nodes in the network. This observation is a result of the approximation made in calculating P_n.

D. Using Partial Trust with Malicious Nodes

In this section, we investigate the effect of employing shared keys for trust between honest nodes in the network. Depending on the type of key pre-distribution scheme, it is likely that an honest node will share keys with some of its neighbors, and not share any keys with some of them. Furthermore, malicious nodes may compromise keys of honest nodes in order to thwart the trust mechanism utilized between honest nodes. The key sharing mechanism for trust and the key compromising probability of malicious nodes may affect what we call "the degree" of a node. This degree refers to the number of neighbors that a node trusts based on shared keys, even though some of them may be malicious. Let η be the probability that two honest nodes share at least one common key and P_m be the probability that an honest node shares a common key with a malicious node in its SISO neighborhood. Then, "the degree" of a node becomes

$$\delta'_s = \delta'_h + \delta'_m = \eta\delta_h + P_m\delta_m.$$

We note that degree $\delta'_s = \delta_s$ when both key sharing and key compromising probabilities are 1, $\eta = P_m = 1$. We analyze successful packet reception with multi-hop SISO and multi-hop vMISO with two different key predistribution schemes: deployment-based scheme [14], and random key pre-distribution [3]. The probability that a node shares a common key with nodes in its neighborhood is larger with the deployment based scheme [14] while it is smaller with the random pre-distribution scheme [3].

TABLE I
DEPLOYMENT BASED KEY PREDISTRIBUTION

		$0 < d \leq d_s$	$d_s < d \leq d_v$
No compromised nodes	η	1	$0 \leq \eta \leq 1$
((7) and (8))	P_m	0	0
With compromised nodes	η	1	$0 \leq \eta \leq 1$
((17) and (19))	P_m	$0 \leq Pm \leq 1$	$0 \leq Pm \leq 1$

1) Using deployment-based scheme: In the case of deployment based schemes, a node may share keys with its neighbors with high probability ($\eta \approx 1,\ 0 < d \leq d_s$), but not with nodes that are far away ($0 \leq \eta < 1,\ d > d_s$). Assuming that an intermediate node is not malicious, in such schemes, it is likely that the complete route is safe. Then, the success probability with SISO is only affected by the fraction of compromised nodes P_m. Let the probability that an intermediate node in SISO range is honest be $\gamma_s = \frac{\delta'_h}{\delta'_s} = \frac{\delta_h}{\delta_h + \delta_m P_m}$ ($\eta = 1$ and $\delta'_s >> 1$). Then, the success probability on a SISO route of length K_s hops is,

$$P_{suc}^{SISO} = (1-p_{out})^{K_s} \times \gamma_s^{K_s-1} \quad (17)$$

In single-hop vMISO transmission, the probability that a source node chooses $n-1$ honest nodes out of δ'_s nodes in SISO range is,

$$P'_n = \frac{\binom{\delta'_h}{n-1}}{\binom{\delta'_s}{n-1}} = \prod_{i=0}^{i=n-2} \frac{\delta'_h - i}{\delta'_s - i}. \quad (18)$$

For multi-hop vMISO, the probability that an intermediate node in vMISO range is honest depends on η and will be $\gamma_v = \frac{\delta'_h}{\delta'_s} = \frac{\eta\delta_h}{\eta\delta_h + \delta_m P_m}$ ($0 \leq \eta \leq 1,\ 0 \leq P_m \leq 1$). Then, the success probability is,

$$P_{suc}^{vMISO} = (1-p_{out})^{nK_v} \times (P'_n)^{K_v} \times \gamma_v^{(K_v-1)}, \quad (19)$$

where in the calculation of P'_n, the key sharing probability is $\eta = 1$, whereas in the calculation of γ_v, the key sharing probability may be $0 \leq \eta \leq 1$.

Now the success probability depends on γ_s and γ_v instead of only γ in addition to p_{out}, n and β. Following the second condition in the proof of Theorem 2, let $\gamma_s = 1 - p_{out}$ and $P'_n \approx \gamma_s^{n-1}$. When we compare (17) and (19):

$$\begin{aligned} P_{suc}^{vMISO} &> P_{suc}^{SISO} \\ \gamma_s^{K_v(2n-1)} \times \gamma_v^{(K_v-1)} &> \gamma_s^{K_s-1} \\ \gamma_v^{(K_v-1)} &> \gamma_s^{K_s-1-K_v(2n-1)} \end{aligned} \quad (20)$$

(20) can be investigated under 3 different cases:

1) When $\eta \to 1$, $\gamma_v \to \gamma_s$; then, vMISO performs better than SISO when $I_v = nK_v - K_s < 0$ as in Theorem 2.
2) When malicious nodes do not have the ability to compromise the keys of honest nodes ($P_m = 0$), $\gamma_s = \gamma_v = 1$

TABLE II
RANDOM KEY PRE-DISTRIBUTION

		$0 < d \leq d_s$	$d_s < d \leq d_v$
Without compromised nodes	η	$0 \leq \eta \leq 1$	$0 \leq \eta \leq 1$
((7) and (8))	P_m	0	0
With compromised nodes	η	$0 \leq \eta \leq 1$	$0 \leq \eta \leq 1$
((17) and (19))	P_m	$0 \leq Pm \leq 1$	$0 \leq Pm \leq 1$

and $P'_n = 1$, and the success probability with SISO and vMISO are the same as (7) and (8) (when there are no malicious nodes in the network), respectively. Then, according to Theorem 1, vMISO is more efficient than SISO when $I_v = nK_v - K_s < 0$.

3) When $P_m \to \eta = 1$ in SISO case, $\gamma_s \to \gamma$; therefore, success probability (17) approaches (10). Similarly, in the vMISO case, when $P_m \to \eta$, $\gamma_v \to \gamma$ and $P'_n \to P_n$; therefore, (19) approaches (12). We recall that (10) and (12) are valid when there is no trust mechanism in the presence of malicious nodes in the network. This is expected when $P_m = \eta$, because the trust mechanism cannot differentiate between malicious and honest nodes.

Table I summarizes the values appropriate for η and P_m when deployment based key predistribution is used to trust nodes with and without the presence of compromised nodes.

2) Using random key pre-distribution: In the case of random key pre-distribution schemes, a node shares keys with its neighbors and with nodes that are far away with equal probability ($0 \leq \eta \leq 1$). Therefore, the success probability of SISO is affected by both key sharing probability of honest nodes, η, and the fraction of compromised nodes, P_m. The success probability with SISO is given in (17) where the probability that an intermediate node in SISO range is honest is calculated from

$$\gamma_s = \frac{\delta'_h}{\delta'_s} = \frac{\delta_h \eta}{\delta_h \eta + \delta_m P_m}.$$

Similarly, in the case of vMISO, P'_n and γ_v are calculated with given $0 \leq \eta \leq 1$, and the success probability is given in (19). Therefore, we can again use (20) for analysis:

1) With random key pre-distribution schemes, $\gamma_s = \gamma_v$. Assuming $P'_n \approx \gamma_s^{n-1}$, vMISO is more efficient if $I_v = nK_v - K_s < 0$.
2) With no compromised nodes $P_m = 0$, $\gamma_s = \gamma_v = 1$ and $P'_n = 1$. Then, following the same analogy as in the case with deployment based schemes, Theorem 2 is valid when random key pre-distribution schemes are employed.
3) When $P_m \to \eta$, $\gamma_s \to \gamma$ and $\gamma_v \to \gamma$; therefore, the success probability (17) approaches (10), and (19) approaches (12). Therefore, Theorem 1 is valid when random key pre-distribution schemes are employed.

Table II summarizes the values appropriate for η and P_m when random key pre-distribution based scheme is used.

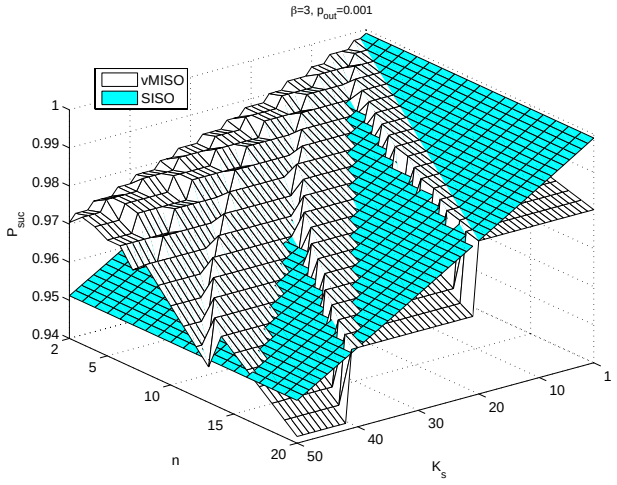

Fig. 4. P_{suc} versus n and K_s, no malicious nodes, $\beta = 3, p_{out} = 0.001$

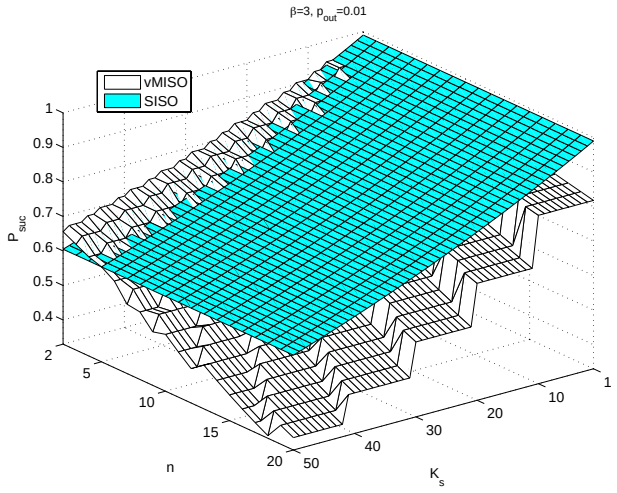

Fig. 5. P_{suc} versus n and K_s, no malicious nodes, $\beta = 3, p_{out} = 0.01$

IV. RESULTS

A. Success Probability Without Malicious Nodes

Figure 4 shows the probability of success with SISO and vMISO transmissions with respect to n and K_s when $\beta = 3$ and $p_{out} = 10^{-3}$. While increasing K_s, d_s is kept the same; therefore, increasing K_s also means increasing the source-destination distance D and the number of vMISO hops K_v. We observe that P_{suc}^{vMISO} is sometimes flat for several SISO hops. This is because the same number of cooperating nodes suffice for covering a few SISO hops. We also see that a smaller number n of cooperating nodes is better when D is small enough to be covered by a smaller number of SISO hops. However, a larger number of cooperating nodes may outperform SISO when the number of SISO hops is large (larger D). A similar behavior is observed also in Figures 5 and 6, where success probabilities with SISO and vMISO are shown for different values of β and p_{out}. This behavior was previously explained in Theorem 1. From these figures,

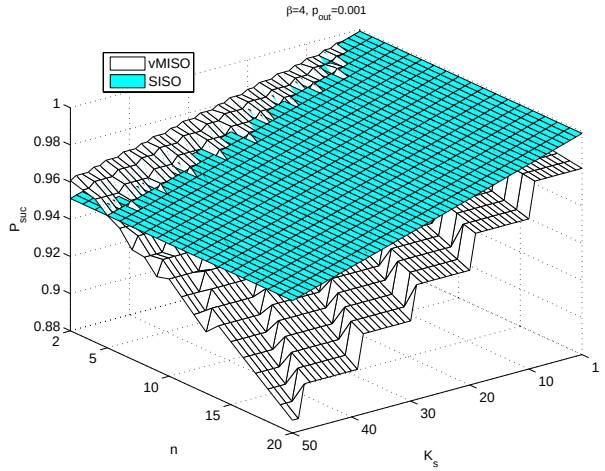

Fig. 6. P_{suc} versus n and K_s, no malicious nodes, $\beta = 4, p_{out} = 0.001$

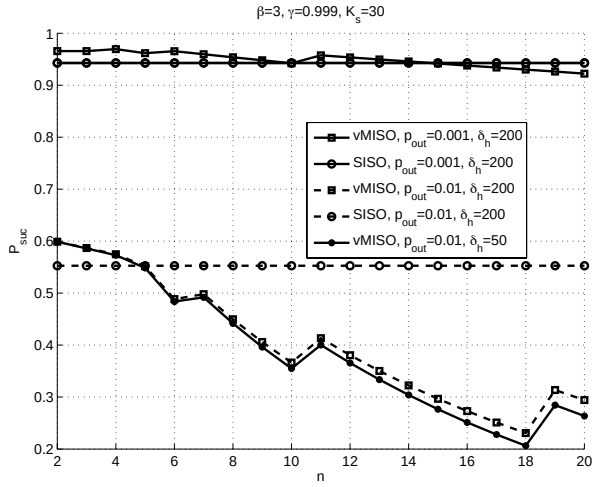

Fig. 8. P_{suc} versus n, with malicious nodes, $\beta = 3, K_s = 30$

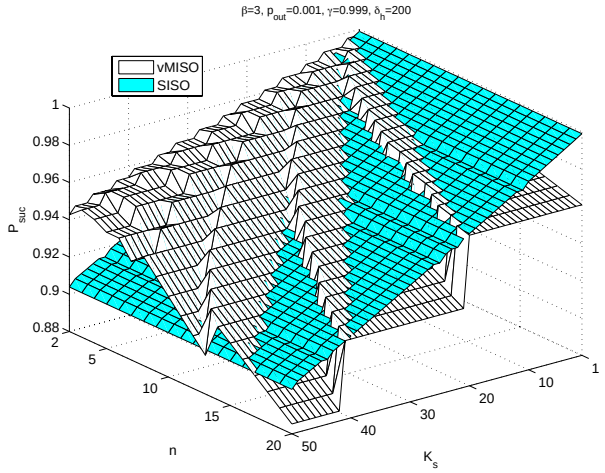

Fig. 7. P_{suc} versus n and K_s, with malicious nodes, $\beta = 3, p_{out} = 0.001$

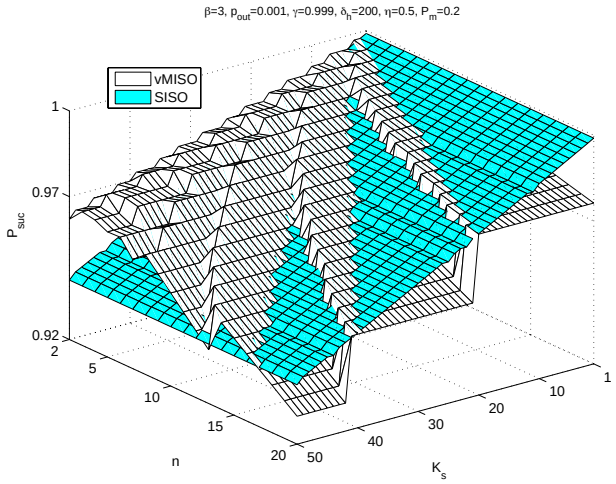

Fig. 9. P_{suc} versus n and K_s, with deployment based key predistribution, $\beta = 3, p_{out} = 0.001$

the success probabilities for vMISO are reduced with higher p_{out} and β. We also observe a reduction in the number of cooperating nodes for vMISO to be more efficient than SISO with larger β although p_{out} is kept the same.

B. Success Probability With Malicious Nodes

In Figure 7, we show P_{suc}^{SISO} and P_{suc}^{vMISO} for various values of K_s and n using (13) and (14). We have picked $p_{out} = 1-\gamma = 10^{-3}$, and used $\beta = 3$ which provides moderate distance gains with cooperative transmissions. Also, a high number of honest node degree is assumed $\delta_h = 200 >> 1$ for approximating $P_n \approx \gamma^{n-1}$. When compared to Figure 4, SISO and vMISO success probabilities decreased approximately by a factor of γ^{K_s-1} and γ^{nK_v-1}, respectively. We emphasize that since p_{out} and β are the same for both cases, the relation between performance comparison are the same for both cases, $I_v = nK_v - K_s > 0$ for n and K_s for higher vMISO success probability.

In Figure 8, P_{suc} with SISO and vMISO are given for $\beta = 3$, $\gamma = 1 - p_{out}$. We pick the distance between the source and the destination nodes as $K_s = 30$ hops to create a scenario to compare the results with $\delta_h = 200$ and $\delta_h = 50$. We observe that the approximation $P_n \approx \gamma^{n-1}$ provides a success probability which is very close to its actual value. Another observation is that with larger p_{out}, the number of cooperating nodes must be small $n < 5$ for vMISO to be better.

C. Success Probability With Key Pre-distribution Schemes

Figures 9 and 10 show the success probabilities when deployment based scheme is employed with $p_{out} = 1 - \gamma = 0.001$. We picked $P_m = 0.2$, and $\eta = 0.5$ for $d > d_s$ in the calculation of P_{suc} with vMISO. The observation is similar to the one seen in Figure 7. In Figure 10, we plot P_{suc} with different η and P_m values when $K_s = 30$ hops and $\delta_h = 50$. When $\eta = 0.5$ and $P_m = 0.5$, an honest node cannot communicate with half of the nodes that reside in its transmission range, and it considers half of the malicious nodes in the

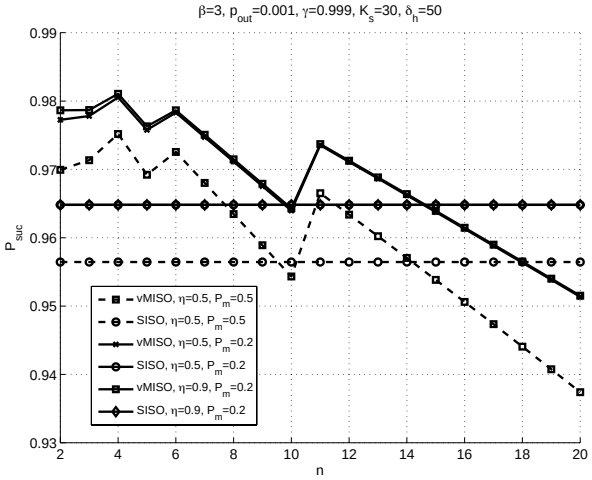

Fig. 10. P_{suc} versus n with deployment based scheme, $K_s = 30$ hops

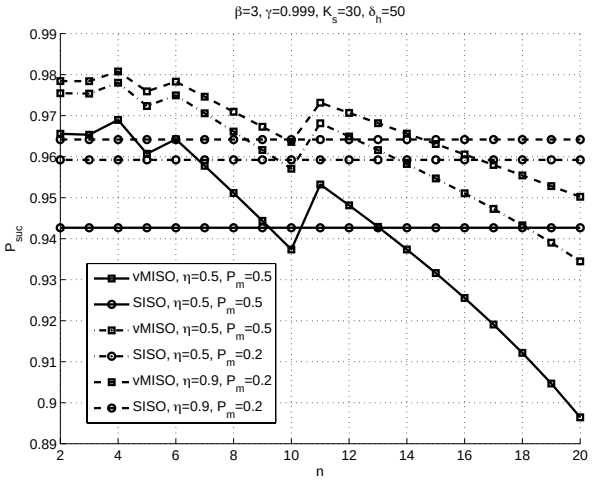

Fig. 11. P_{suc} versus n and with random key pre-distribution, $K_s = 30$ hops

neighborhood as honest nodes. Therefore, this case has a lower success probability compared to those achieved with $\eta = 0.5$ and $P_m = 0.2$ and $\eta = 0.9$ and $P_m = 0.2$.

Exactly the same scenario was created with random key pre-distribution, and the results are shown in Figure 11. When $\eta = 0.5$ and $P_m = 0.5$, the success probabilities are lower than those with deployment based scheme due to the reduction in "presumably honest node degree" in SISO range with random key pre-distribution. The highest success probabilities for given parameters are achieved when $\eta = 0.9$ and $P_m = 0.2$ as expected. We also see that the best number of cooperating nodes is $n = 4$ for the scenario considered in Figures 10 and 11. When $n = 4$, $G_n(p_{out}, \beta) = 7.5381$ and $I_v = nK_v - K_s = -14 < 0$.

V. Conclusions

Cooperative transmissions exploit a fundamental feature of the wireless medium: the ability to achieve diversity through independent channels created between the multiple transmitters and the receiver, because these channels are likely to fade independently. With more relay nodes, a higher order of diversity can be achieved improving the BER and/or transmission range. However, at the same time, cooperative transmissions suffer from drawbacks from a security point of view due to the involvement of additional parties to the communication. In this paper, we evaluate the tradeoffs between using cooperative transmissions or not for reliable transmission of packets in sensor networks with a mix of honest and malicious nodes. We showed that when the number of honest nodes in the neighborhood of a node is much higher than the number of cooperating nodes (n), at high outage probability, vMISO with small n outperforms SISO in terms of successful transmission probability. We also derived a general condition (under simplifying approximations) for all cases where vMISO outperforms SISO.

Acknowledgments

This work was funded in part by the Army Research Office MURI grant W911NF-07-1-0318.

References

[1] G. Jakllari, S. V. Krishnamurthy, M. Faloutsos, P. Krishnamurthy, and O. Ercetin, "A framework for distributed spatio-temporal communications in mobile ad hoc networks," *Proceedings of Infocom*, 2006.

[2] A. Aksu and O. Ercetin, "Reliable multi-hop routing with cooperative transmissions in energy-constrained networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 8, pp. 2861–2865, August 2008.

[3] L. Eschenauer and V. D. . Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the 9th ACM Conference on Computer and Communications Security (Washington*, U. DC and N. V. Atluri, Eds. New York, NY, 41-47: CCS '02. ACM, 2002, pp. 18–22.

[4] J. N. Laneman, "Cooperative diversity in wireless networks: Algorithms and architectures," Ph.D. dissertation, Massachusetts Institute of Technology, Cambridge, MA, August 2002.

[5] S. Haykin and M. Moher, *Modern Wireless Communications*. Prentice Hall, 2005.

[6] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE Journal on Select Areas in Communications*, pp. 1451–1458, October 1998.

[7] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1456–1467, July 1999.

[8] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *Trans. Wireless. Comm.*, vol. 8, no. 10, pp. 5003–5011, 2009.

[9] E. E. A. Sendonaris and B. Aazhang, "User cooperation diversitypart i: System description," *IEEE Transactions on Communications*, vol. 51, no. 11, p. 19271938, November 2003.

[10] X. He and A. Yener, "Two-hop secure communication using an untrusted relay: A case for cooperative jamming," *IEEE Globecom*, 2008.

[11] Z. Han and Y. L. Sun, "Securing cooperative transmission in wireless communications," *Proc. Mobiquitous*, 2007.

[12] W. Yu and K. R. Liu, "Secure cooperative mobile ad hoc networks against injecting traffic attacks," *Proc. IEEE SECON*, 2005.

[13] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *SP '03: Proceedings of the 2003 IEEE Symposium on Security and Privacy*. Washington, DC, USA: IEEE Computer Society, 2003, p. 197.

[14] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A key predistribution scheme for sensor networks using deployment knowledge," *IEEE Transactions on Dependable and Secure Computing*, vol. 3, pp. 62–77, 2006.

[15] A. Paulraj, R. Nabar, and D. Gore, *Introduction to Space-Time Wireless Communications*. Cambridge: Cambridge University Press, 2003.