Network Coding Based Security for Routing Attacks in WRN: Frechet Interference and Rayleigh Outage Evaluation

R. Villalpando-Hernández*[1], C. Vargas-Rosales[2], D. Muñoz-Rodríguez[2], J. R. Rodríguez[2]

[1] Instituto Tecnológico y de Estudios Superiores de Monterrey Campus Laguna
Paseo del Tecnológico #751, Col. Ampl. La Rosita, 27250.
Torreón, Coahuila, México
rafaela.villalpando@itesm.mx
[2] Instituto Tecnológico y de Estudios Superiores de Monterrey Campus Monterrey
Eugenio Garza Sada #2501, Col. Tecnológico, 64849.
Monterrey, Nuevo León, México

ABSTRACT
We present a network coding security method capable of detecting several routing attacks in wireless reconfigurable networks. Routing security attacks include selective forwarding, black holes, and wormholes. The proposed method performs linear network coding over intermediate nodes composing a given route, not only to distribute content, but also to provide data confidentiality by cooperation as a mechanism of detection. The method presents a robust, accurate and fast response under security attacks for varying network conditions, such as interference and outage due to channel fading. It also provides a gain in network throughput by increasing the number of successfully received packets without a significant increase of the bandwidth usage.

Keywords: Network coding, sinkholes, selective forwarding, Frechet, outage.

RESUMEN
Presentamos un método basado en codificación de red capaz de detectar ataques de seguridad a la información de ruteo en redes inalámbricas reconfigurables. Los ataques de seguridad a la información de ruteo incluyen ataques como el envío selectivo de datos, agujeros negros y gusanos. El método propuesto realiza una codificación de red lineal en los nodos intermedios de una ruta determinada, para distribuir datos y para proveer confidencialidad por medio de un mecanismo cooperativo de detección. El método presenta una respuesta robusta, rápida y precisa ante ataques de seguridad bajo condiciones de red variables, tales como interferencia y pérdida de comunicación debido al desvanecimiento del canal. También incrementa los datos que llegan al destino sin incrementar significativamente el uso del ancho de banda.

1. Introduction

Wireless Reconfigurable Networks (WRN) are characterized by their capability to rapidly change their topology in order to adapt to current network needs without the use of infrastructure. In WRN, security becomes a requirement where data integrity and confidentiality must be protected from a variety of attacks. Current security schemes are based on cryptography, providing a partial and expensive (high processing) defense since they usually rely on a central unit, which results inconvenient for mobile networks. We propose a Detection and Defense Method (DDM) that provides an innovative and inexpensive processing alternative that uses network coding not only to collaborate in packet distribution,but also as a tool for monitoring and detecting several attacks.

The DDM is based on random network coding, [1]. Routing with network coding, involves cooperative processing from the nodes in the route. The DDM solves attacks such as the Sinkhole where an intruder attracts network traffic by advertising itself as having a better path from a source to a destination. Also, *Selective forwarding* where once an adversary creates a sinkhole, it refuses to forward a selection to the destination.

The DDM is evaluated throughout simulations under realistic network conditions such as Frechet

interference and outage due to Rayleigh channel fading. These are important issues since they limit network capacity and grade of service. From the point of view of data integrity, errors can be caused by interference instead of security attacks. On the other hand, the DDM is based on the existence of a set of routes considered trustable; therefore, it is important to make an estimation of how reliable such routes are based on an outage probability analysis.

2. Related work

There are several mechanisms proposed which attempt to solve routing security problems. Recently, [2] presented a central processing algorithm to detect an intruder in a sinkhole attack. This algorithm finds a list of suspected nodes and carries out a network flow graph identifying a sink attack by observing data missing from an attacked area. They perform evaluations in a free interference or fading network. In a different setting, [3] presents a scheme that uses node collaboration and data redundancy to solve attacks associated with data authenticity and availability. They assume that at least one node can recognize a single event and broadcast it to multiple nodes. They use network coding for generating random linear combinations of the packets they receive. In [4], authors consider a random network coding scheme where source nodes include in each source packet hash symbols calculated as polynomial functions of the source data. Receiver nodes check the data and hash values of their decoded packets to determine if data has been modified. Simulations under realistic networks are not provided. We present in [6] and [7], the formulation of the DDM in WRN. In [6], an analysis of the method under a heuristic measure of interference is presented. In [6], the DDM detects an attack taking into consideration that data modification can also be caused by an interference factor in the route. The interference factor is obtained by the relation of the maximal interference of a node in the route to the maximal interference of a node in the network. Interference measure is based on the number of nodes in an interference area defined by a disk of a given radius. Also in [6], an analysis of the threshold packets for attack recognition is commanded. In [7], we introduce an interference analysis based on the Nearest Neighboring Node, [5], and an outage probability analysis, and evaluate the DDM under a basic scenario. In [8], network coding is used to increase multicast capacity in a mechanism based on an encryption key and a checksum to provide confidentiality and integrity in a network. The authors do not use network coding as a tool in order to provide security; they propose a mechanism suitable for network coding environments. The proposed mechanism encrypts data packets and use linear operations for checksum. Simulations for attack probabilities (.05 to .4) are provided where the number of successfully received packets is analyzed. It will be shown that the mechanism proposed in this paper presents a better performance (about 60% for attack probability of 0.4) for higher attack probabilities than that in [8] (about 20% for attack probability of 0.4).

In this paper, we introduce different network parameters that provide us a different viewpoint of the DDM, showing tradeoffs between node density and interference. We also evaluate the tradeoff between transmission range and outage probability. At the same time, we discuss how the DDM provides a robust behavior for node mobility and an adversary with dynamic capabilities.

3. Model description

Consider a WRN where a set of nodes are randomly placed in an operational area A. Each node is allowed to command network coding. We assume that *trustable* routes [6] are already available. Figure 1 shows the scenario where we have a trustable route in operation R_t: s, 1, 2, 3, 4, *d*, from source *s* to destination *d* and another node announces a new route as a better option, i.e., R_{new}: s, 1, 5, 4, *d*. This node 5 might be an intruder that is able to monitor trustable routes in order to command a sinkhole or selective forwarding attack announcing itself as a better route than the existing one. If we assume unitary costs in every link (Figure 1), the trustable route has a higher cost than that of the new route.

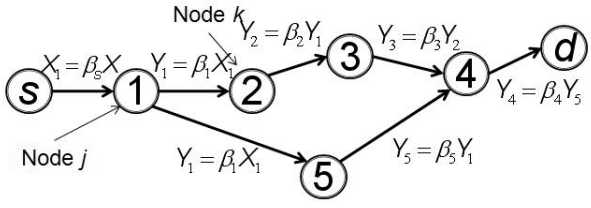


Figure 1. Network topology: typical change.

3.1 Network Coding

Consider the network as a directed acyclic graph *G*. The packets under transmission in the network are seen as a set of discrete independent random processes $X_1, \ldots, X_r$. The packets are observable at one or more source nodes $m \geq 1$, and there are $d \geq 1$ receiver nodes. The random process carried by edge $e_{j,k}$ that starts in node *j* (i.e. *j*=1 in Figure 1) and ends at node *k* (i.e. *k*=2 in Figure 1) is denoted Y_j. We assume that information is transmitted in packets with constant length *l*. In a linear code, Y_j is a linear combination of incoming information flows this is $Y_j = \sum_s \beta_s X_s + \sum_{k \in I(j)} \beta_k Y_k$, [1], where information is coded by a random linear coding coefficient given by β_k for node *k*. Note that $\beta=\{\beta_1, \beta_2,..,\}$ is the set of local encoding coefficients whose values can be strings taken from the set $\{\pm 1\}$. Therefore, an information flow from source X_s coded by β_s, can be expressed as $\beta_s X_s$, therefore, if the flow is coded by another node *j* with code β_j, the resulting flow will be $\beta_j \beta_s X_s$.

Let us assume that the initialization phase where trustable routes are discovered and stored in a database can be performed, [6]. After this phase, and due to mobility of nodes, some routes may change and scenarios such as that presented in Figure 1 may be present over the network.

When some trustable node k detects a second route with lower cost, see node 1 in Figure 1, then this node k sends the packet information from s to d over the two routes in order to enable the DDM. Note that if the trusted route cannot be maintained due to issues such as mobility or interference, then the nodes can find another trusted route from s to d according to the current network conditions. This can be done as long as a trusted route can be found.

3.2 Detection and Defense Method (DDM)

We analyze the problem when a change is caused by an existing node in the network that announces a new route as an alternative to a one already trustable route. Once the compromised node achieves the change of route, it can command a sinkhole and a selective forwarding attack. When network coding is allowed, we assume that intermediate nodes do not introduce extra data. Figure 1 shows the random network coding information flow in a classic topology. As stated before, node 1 detects that it has to send the coded information over two routes, thus starting the DDM, and sends to node 2 an alarm message which propagates to the rest of the nodes in the trustable route.

First, let us divide the operation of the DDM in iterations i_k, [7], as shown in Figure 2. Second, there is an operation related to every i_k (Figure 3). Also, we suppose that two nodes can be transmitting in the same iteration without causing interference to each other. The performance measures are the following; For Figure 2 and Figure 3, the DDM works as follows. In Figure 3 a), we can observe that from i_1 to i_3, X_1 is generated by source *S*, transmitted and received by node n_1, where it is also coded. In Figure 3 b), actions performed from i_4 to i_9 are explained, several actions take place at the same time because information packets are sent through both, the trustable and the suspicious route. Node 4 receives Y_3 and Y_5, and requests to the suspicious node 5 its coding coefficient β_5. Thus, node 5 sends its coding coefficient, assume that this is $\beta_5^{'}$. Then node 4 processes the detection packet $W_4 = Y_3 Y_5 \beta'_5$, where $Y_3 = \beta_s \beta_1 \beta_2 \beta_3 X$ and $Y_5 = \beta_s \beta_1 \beta_5 X$. Therefore, $W_4 = (\beta_2 \beta_3 \beta_5)\beta_5^{'}$, if $\beta_5 = \beta_5^{'}$, then $\beta_5 \beta_5^{'} = 1$ and $W_4 = \beta_2 \beta_3$. In Figure 3 c), we can observe that W_4 is sent to node 3, which processes $W_3 = W_4 \beta_3 = (\beta_2 \beta_3)\beta_3 = \beta_2$, and sends it back to node 2, producing $W_2 = W_3$ $\beta_2 = (\beta_2)\beta_2 = 1$. Following this formulation, we can see that if β'_5 is the original coding coefficient used by node 5, then, node 2 verifies that $W_2=1$ validating the new route; otherwise node 2 obtains that $W_2 \neq 1$ disabling the new route and classifying node 5 as an intruder node. Furthermore, packet transmission continues over the trustable route. In this approach, we can see b'_k as the public key of node *k* that can be known by any node in the network. In Figure 2, we show in detail all the iterations performed in a communication session commanding the DDM, where three different processes are commanded in parallel. The first one, when information is sent from *s* to *d* throughout the new route (Figure 2c). The second

one throughout the trusted route while the DDM is being executed (see Figures 2a and 2b). The third one and final one is the sending of β'_5 by node 5 in order to complete the DDM (Figure 2d).

3.2.1. Packet Overhead

In order to validate an attack throughout the new route, the DDM keeps working on the trustable route until the attack is detected, if no attack is detected, then the DDM will be operating until a *threshold* α is achieved. For the general case, the packet overhead is given by $\rho_X = 2l_{1,j} - 1$, where $l_{1,j}$ is the length from node 1 to node j (i.e. j=3 in Figure 2) [6]. The packet overhead ρ_X can be seen as the cost imposed by the DDM to the network.

3.3 DDM Performance

In this section, two important parameters used to evaluate the DDM performance are presented.

3.3.1. Successfully Received Packets

The number of packets received successfully is affected by the time that the DDM takes to validate an attack because in such time iterations packets are being sent over the route to be validated (new route). Let us define X1j as the packet generated by the source at iteration ij. For the network, in Figure 2, the DDM is able to detect an attack up to iteration i15. The packets exposed to the attack from node 5 are those produced by s from i1 to i13 because packets X114 and X115 have not reached node 5 at i15, therefore, these packets can be redirected if necessary. The procedure illustrated in Figure 2 can be extended to the general attack case given in Figure 1. As stated in [6] the number of packets exposed to attack is given by $\Delta X = 2[l_{s,j} + (l_{j,1} - 1)]$, where $l_{s,j}$ and $l_{j,1}$ are the length in hops of the forward route from s to j, and the backward route from j to node 1, respectively, in Figure 1, node j is node 1. ΔX denotes the number of packets that are sent through the new route while the DDM verifies if the new route is a good or a bad route; therefore, if it is a bad route, then ΔX packets may be lost or modified by the attacker while the DDM disables the new route. ΔX indicates how efficiently the DDM can detect an attack from the new route.

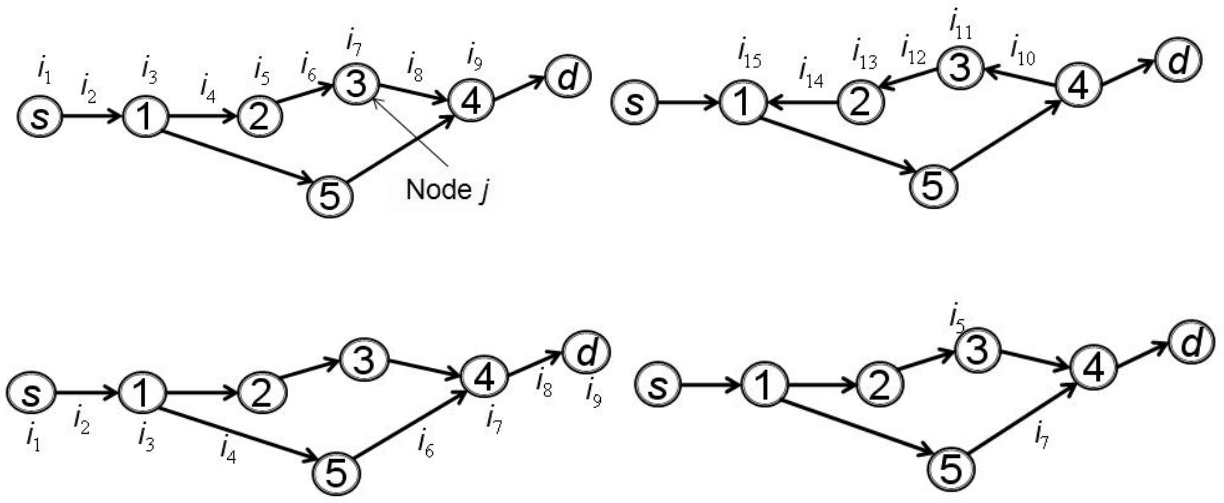


Figure 2. Iteration consumption for attack validation.

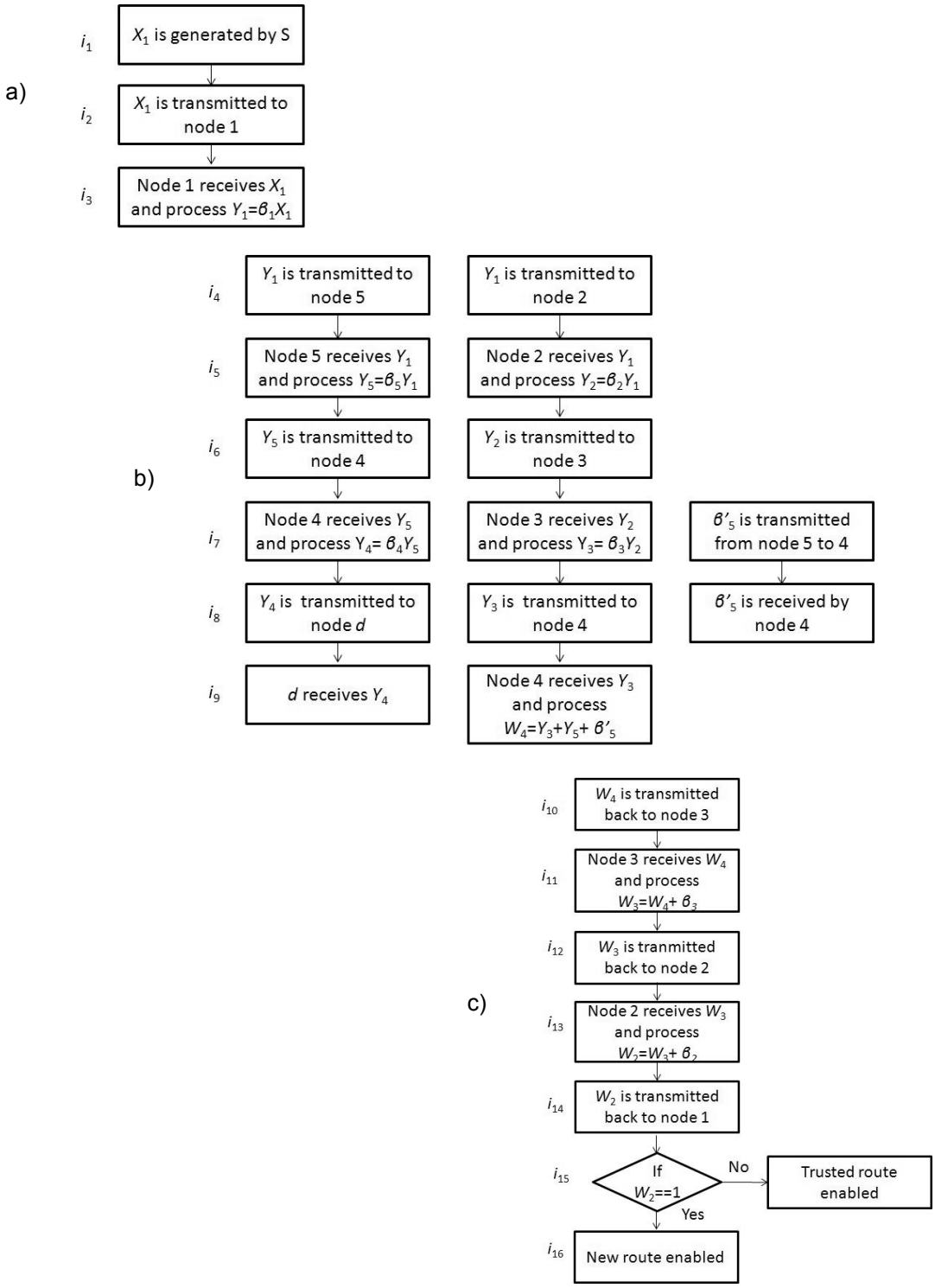


Figure 3. Operations realized in each iteration by the DDM.

3.3 Network Impairments

In WRN, several impairment factors degrade transmissions causing packet loss. Now, we extend the environments where interference can cause packet loss. Also we consider outage probability of the trusted route (probability of unreliable route).

3.4.1. Frechet Interference

We present the Nearest Neighboring Node (NNN) interference analysis since it is the node with the most influence. The NNN interference of a WRN can be characterized by its cumulative distribution function (cdf) and its probability density function (pdf). The pdf of the NNN interference is given by a Frechet distribution, [5], considering a 2-D region. Assume that every node uses a constant transmission power, P_T, which is determined by the amount of dBm's that must be received at a distance r_{max} by a node in order to maintain communication. Thus, the maximum *coverage* region that a node has must be of r_{max} meters, distance at which its signal must be received at a power P_R [5], With P_T=$P_R r^{\gamma}_{max}$, (γ is the path loss) assuming that the NNN transmitting at the same time is located at an exponentially distributed distance D from the reference node, interference I_f experienced is characterized by $F_{If}(\eta) = e^{-\lambda\pi(P_T/\eta)^{2/\gamma}}$, where λ is the node density, of a Poisson spatial process. The pdf is given by $f_{If}(\eta) = \frac{2\lambda\pi}{\gamma P_T}\left(\frac{P_T}{\eta}\right)^{2/\gamma+1} e^{-\lambda\pi(P_T/\eta)^{2/\gamma}}$. It can be seen that $F_{If}(\eta)$ and $f_{If}(\eta)$ correspond to the cdf and the pdf, respectively, of a random variable with Frechet distribution, [5]; therefore interference caused by the NNN transmitting at P_T is a stable Frechet pdf with shape parameter $\zeta = 2/\gamma$, and scale parameter $\sigma = \lambda\pi^{\gamma/2}$ and variable $x = \eta$.

Therefore, DDM has to identify if a packet has been modified or lost due an attack or due to interference. We follow the same procedure as that in [6] but define differently p_I, the probability that a packet will not be correctly received at the destination due to interference. Based on the NNN interference analysis, we set p_I as $(I_f \le \eta)$, which is known, if we know the distance of the nearest neighboring node to any node in the path of the trustable route (Figure1). We establish that if Pr $(I_f \le \eta)$ is above the threshold probability p_t, then the packet is not correctly received due to interference. As a first approach, we select p_t randomly in order to simulate heterogeneous quality of service conditions for nodes in the network. Let us define p_a as the probability of routing security attack. The error probability p_e, is the probability that the packet will not be received correctly for any reason and is defined as $p_e = p_I p_a + (1 - p_I)p_a + p_I(1 - p_a)$.

3.4.2. Outage Probability.

An outage evaluation based on fading channel state and source-destination distance as proposed in [9] is commanded. Assuming rich scattering where the Rayleigh fading model and node distribution according to a Poisson process are allowed, we can use the outage model proposed in [9]. We use Rayleigh instead of Ricean fading because in ad-hoc scenarios, nodes transmit in an omnidirectional way, therefore transmissions find several objects on which they can bounce including other nodes' devices. This situation implies that node-to-node communication will not necessarily be on a 100% line-of-sight path and will be accompanied by multipath components. Thus, Rayleigh fading is included in the simulations, which is also for slow fading channels, this is, channels with changes faster than a packet transmission time but slower than the symbol duration.

Let us assume that every node is able to use a constant transmission power, P_T. Let d be the distance between transmitter and receiver and d_n be the distance d to the n-th nearest neighbor in a sector ϕ. Also $(SNR)_{Tx}$ can be defined as P_T/N, where N is the power of noise. The outage probability is defined as follows when the received SNR is less than the defined threshold ε in a given condition of distance D. The outage probability is given by $P_o = 1 - \left[\frac{\varphi/2}{\varphi/2 + \varepsilon/(SNR)_{Tx}}\right]^n = 1 - B^n$, where n is the number of hops in the route [9]. In a relay system, an outage occurs if either one of the links is in outage. The outage probability for a relay routing which has n-1 hops from source to destination is given by

$$P_{n,out} = 1 - \left(1 - P_{n-1,out}\right)\left(1 - P_{(n-1)n,out}\right) = 1 - B^{n-1}$$

where $P_{ij\ ,out}$ is the outage probability that the message is transmitted unsuccessfully from node *i* to node *j* .

Based on this formulation, we are able to evaluate if a trusted route is reliable in order to command the DDM. If $P_{n,out}$ is below to a outage probability threshold p_o then the actual trusted route is considered unreliable and another trusted route is found.

3.4.3. Attack Detection Rule.

Two measures are taken by the DDM in an attack detection process. First, the DDM will modify the *threshold* α to recognize if the attack has been performed. This threshold is given by $\alpha = C\lceil p_I \Delta_X \rceil$, where *C* is a proportionality constant and $\lceil \ \rceil$ is the ceiling function. Second, we establish a detection rule. Throughout simulations, we obtained that 80% of the threshold α needs to be received correctly in order to declare that no attack has been commanded. If the DDM declares that no attack has been commanded, the new route is used and the DDM activates a monitoring process with probability p_m. This monitoring process commands the DDM over a trustable route available. The monitoring probability p_m is given by the ratio of the incorrectly received packets and the total packets received in the last 20% of α . In Table 1, the definition of all the parameters of the model is provided.

Parameter	Definition
p_X	Packet overhead
Δ_X	Number of packets exposed to a security attack
r_{max}	Maximum transmission range
P_R	Received power
P_T	Transmitting power
γ	Path loss
I_f	Interference experienced by a node
λ	Number of nodes
μ	Node density
p_I	Probability that a packet will not be received correctly due to interference
p_t	Interference probability threshold
p_e	Error probability
p_a	Security attack probability
$P_{ij\ ,out}$	Outage probability. Probability that the message is transmitted unsuccessfully from the node *i* to the node *j*.
p_o	Outage probability threshold
A	Attack recognition threshold
C	Proportionality constant
p_m	Attack monitoring probability
A	Network area
$(SNR)_{T_x}/\varepsilon$	Signal to noise ratio compared to a threshold ε in dB
ϕ	Sector of the coverage region in radians

Table 1. List of Model Parameters.

4. Results

In this section, we evaluate the performance of the DDM under NNN interference and outage probability given by a Rayleigh fading channel. Our simulations have the base environment of a network scenario with μ nodes which are uniformly distributed in a square area of A=10,000m^2. We suppose a homogeneous transmission range $r_{max}=r$. Also, the path exponent γ=2 and the node density $\lambda = \mu/A$. P_R=100dBm for the interference calculations as done in [5]. For the outage probability, we set ϕ=π/2, and $(SNR)_{T_x}/\varepsilon$ =26dB, as in [9].

We select randomly source and destination nodes and find the shortest route (trusted route) between them if it exists, then the adversary is introduced with the new route. When both routes exist, the outage probability analysis is performed. If one of the two involved routes is not reliable ($P_{n,out} < p_o$) then another route is found. Every time a new route is found node mobility is introduced. Then, we proceed to calculate the interference of the given route p_I as explained before. We evaluate the DDM for this scenario under different attack probabilities p_a and different transmission ranges r. The metrics used for evaluation are the following. Packet Overhead (PO) is defined as the ratio of the total communication overhead in the network commanding the DDM to a network that does not. Successfully received packets (SRP) are defined as the ratio of the number of packets sent by source s to the number of packets received by the destination d, without retransmission. Detection Rate (DR) is the ratio of the number of authentic attacks detected by the DDM to the number of authentic attacks commanded by an adversary. False Positive Rate (FPR) is defined as the ratio of the number of false declared attacks to the total detected attacks. False Negative Rate (FNR) is a measure defined as the ratio of real attacks undetected to the total detected attacks. No Applicability Rate (NAR) is defined as the ratio of the number of times that the DDM is no longer applicable due to the lack of a trusted or a new reliable route to the number of times that a reliable route is found.

In [7], a cost-gain analysis of the DDM was presented by analyzing the PO and the %SRP given by the DDM by plotting p_a against these parameters in a network where interference and outage were not considered. It was shown that the PO caused by the DDM can be and the %SRP obtained with the DDM can be improved as C is decreased. However, the accuracy of the DDM given by the %DR and %FPR are worse as C is decreased. In this paper we set C=2 in order to obtain the improvement in the PO and the %SRP without scarifying the %DR and the %FPR. Also in [7], a basic evaluation of the DDM under NNN interference and Rayleigh outage was done for a network of 100 nodes observing that the %SRP was increased from 10% without the DDM to more than 70% with the DDM .

In the following scenarios, we introduce an adversary with dynamic attack capabilities, by introducing a maximal attack probability $p_{a_{max}}$, i.e., the adversary can chose a different attack probability in the range $0 \le p_a \le p_{a_{max}}$. We present a node density and transmission range analysis for the DDM under NNN interference and outage relaying routing.

In Figure 4a, we consider a network with μ=50 and vary r from 20m to 35m and we observe that we can improve the %SRP if r is increased. It can be seen, however, that for some p_a 25m is sufficient. In Figure 4b, a large network with μ=300 is presented and r is modified from 5m to 25m and we also obtain a %SRP improvement if r is increased, but only for ranges below 25m. This can be explained because when r is increased, the interference in the network is also increased, therefore, there is a tradeoff between the %SRP improvement and the NNN interference. We can also see that the best performance is attained for μ=300.

In Figure 5a, we consider μ=50 nodes and command the range analysis for the PO, with Figure 5b (μ=300), we complete the node analysis for the PO given by the method. In both analyses, we observe that we can achieve an improvement on the PO by increasing r until a threshold is exceeded and the NNN interference grows sufficiently to degrade the PO. A natural explanation for this result may be that using a large r, the routes obtained may be shorter which naturally decreases the number of packets sent in the system. However, this improvement can no longer be maintained when r is large

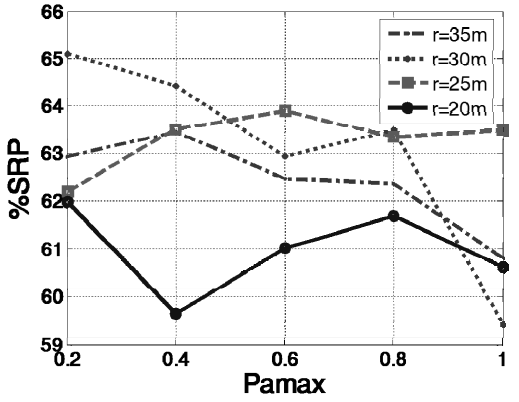
enough to cause high NNN interference which may degrade the system performance. Also, it can be observed that increasing the number of nodes helps decrease the PO, which is a desired result.

In Figure 6a, we set μ=50 and evaluate for r=20m to r=35m. We can observe that the detection capability of the method is not substantially modified as we increase r. On the other hand, in Figure 6b, we set μ=300 and observe results for r from 5m to 25m and we can observe a consistent improvement of the %DR for $p_{a_{max}} \leq 0.6$ that is achieved by decreasing r. However, such improvement cannot be maintained for large ranges like 20m and 25m. This can be explained as follows. Using a short r relies on large routes, which may imply an increment on Δ_X. Large routes also imply large outage probability. Therefore, we also have a tradeoff between range decrease and outage probability. On this basis, we corroborate that by increasing the node density, the DDM detection capability is not sacrificed (r=20m).

In Figure 7a and Figure 7b, we make a range analysis of the %FPR for a network with μ=50 and μ=300 respectively. In Figure 7, we can observe that by decreasing r we can improve the %FPR, this result can be seen clearly for $p_{a_{max}}$=0.2. This result is explained by the same arguments as those used for results in Figure 6. We can also observe that by increasing μ from 50 to 300, the positive false alarms given by the method does not change substantially.

In Figure 8a, we can see that as r is decreased we can obtain a decrement on the %NAR which implies an increment on the probability of finding a suitable route to command the DDM. In Figure 8b, we consider a network with μ=300 and we observe a similar behavior with μ=50 from r=10m to 25m; i.e., as we increase r we obtain a decrement on the %NAR. However, there is a point in which it is not possible to keep improving the %NAR as we decrease the range. This is explained due to the outage probability, as we decrease r we increase the route length, and therefore, the outage probability. Thus, there is a tradeoff between range decrease and outage probability.

a)



b)

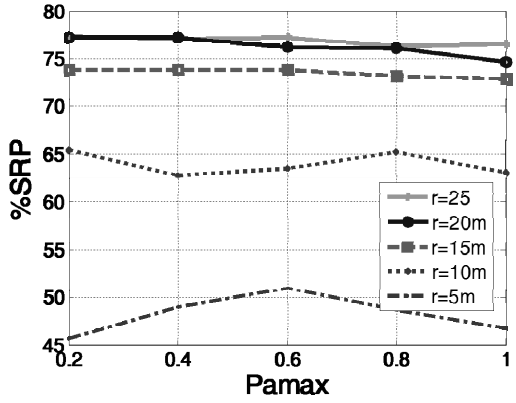


Figure 4. a) %SRP vs. $p_{a_{max}}$, μ=50. b) %SRP vs. $p_{a_{max}}$, μ=300.

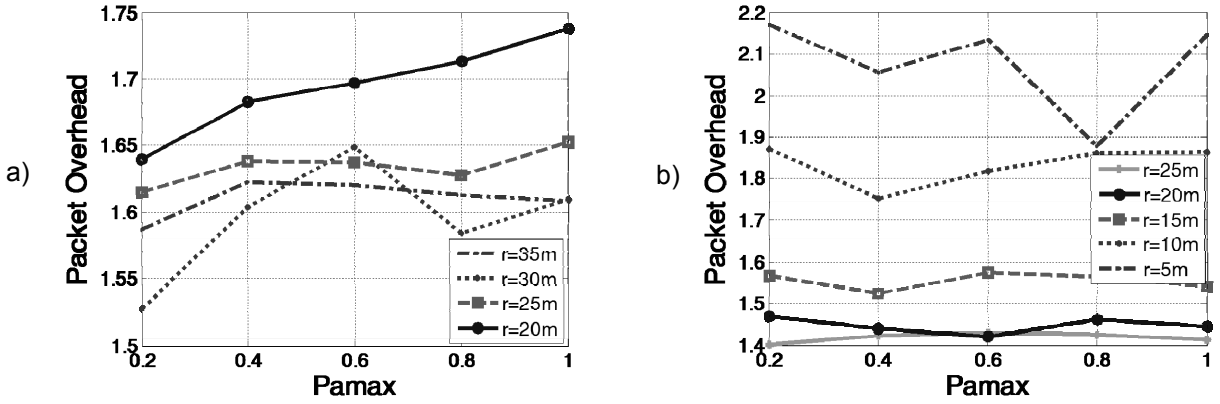


Figure 5. a) PO vs. $p_{a_{max}}$, μ=50. b) PO vs. $p_{a_{max}}$, μ=300.

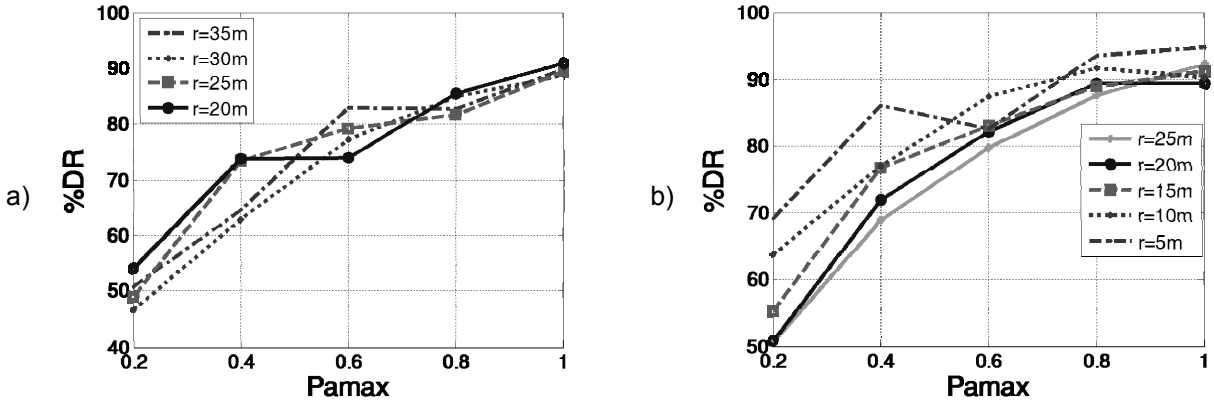


Figure 6. a) %DR vs. $p_{a_{max}}$, μ=50. b) %DR vs. $p_{a_{max}}$, μ=300.

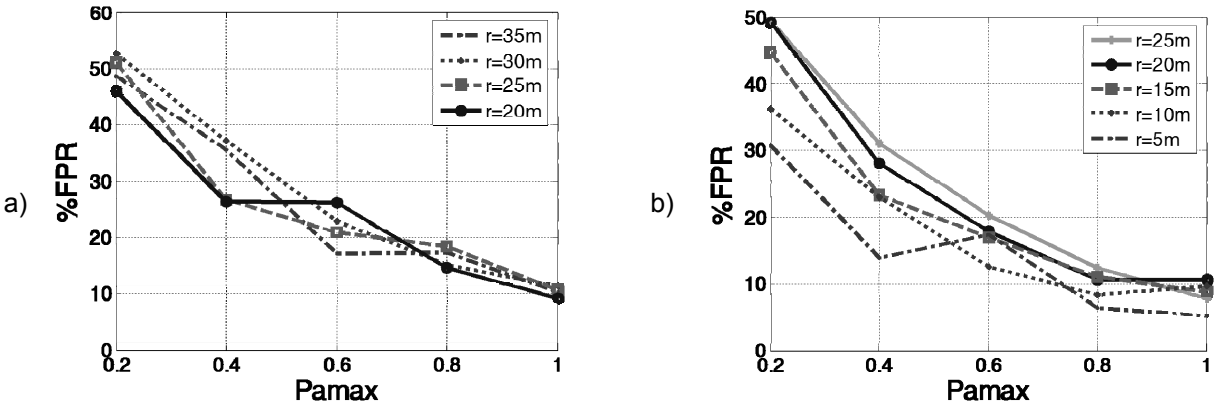
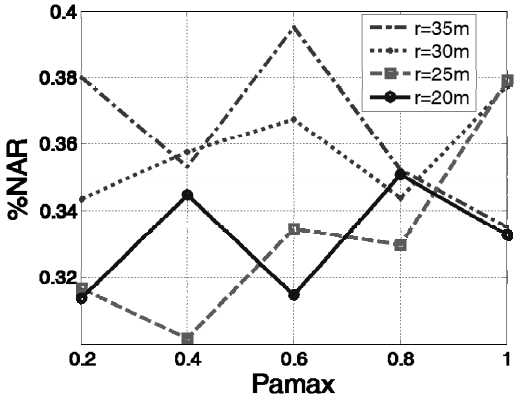


Figure 7. a) %FPR vs. $p_{a_{max}}$, μ=50. b) %FPR vs. $p_{a_{max}}$, μ=300.

a)



b)

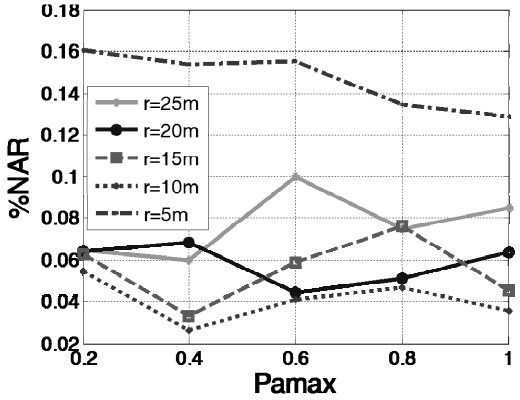


Figure 8. a) %NAR vs. $p_{a_{max}}$, μ=50. b) %NAR vs. $p_{a_{max}}$, μ=300.

Note, that simulations for μ=300 nodes, r=30m and 35m where performed for all the network parameters and behavior resulted similar to that presented for r=25m, for that reason those results are not included.

5. Conclusions

We have presented a distributed and effective method for detection and defense mechanism from sinkhole and selective forwarding attacks in WRN that present channel interference and channel fading. The DDM assumes a basic knowledge of the network topology, the availability of a trusted route, and the capability of every node in the route to command linear network coding over the information. We also formulate an NNN interference analysis and an evaluation of the outage relaying route of a network that performs the DDM. We present a realistic interference and outage analysis under mobility conditions of the DDM for dynamic capabilities of the network adversary. The DDM is evaluated under different node densities and transmission ranges. The main difference between this work and those presented in [6], [7] and [8] is that in this paper we present an exhaustive analysis of the method under more diverse scenarios where the impact of the number of nodes and the transmission range are discussed in more detail. Also, compared with work in [8], we provide analysis for larger attack probabilities attaining better results than those that they report.

Results have demonstrated the accuracy of the algorithm under severe interference and outage conditions imposed by the NNN interference and by the outage relaying route models. Even more, it has been demonstrated that the PO and the %SRP are improved as the node density and transmission range are increased without compromising the accuracy capabilities of the DDM. This is a desirable behavior for large and dense networks.

References

[1] Ahlswede, R., Cai, N., Li, S., and Yeung, R., Network information flow, IEEE Trans. on Information Theory, vol. 46, No. 4, pp. 1204–1216, 2000.

[2] Ngai, E. C. H., Liu J., and Lyu, M. R., On the intruder Detection for Sinkhole Attack in Wireless Sensor Networks, Proc. IEEE ICC, 2006.

[3] Ayday, E., Delgosha F., and Fekri, F., Location-Aware Security Services for Wireless Sensor Networks using Network Coding, IEEE INFOCOM, pp. 1226-1234, 2007.

[4] Ho, T., Leong, B., Koetter, R., Médard, M., Effros M., and Karger, D.R., Bizantine modification detection in multicast networks using randomized network coding, Proc. IEEE International Symposium of Information Theory, pp. 114, 2004.

[5] Vargas, C., Munoz, D., Antonio, M. Z., Modeling Interference in Wireless Ad hoc Networks. Technical Report CET 06-01.

[6] Villalpando, R., Vargas, C., Munoz, D., Network Coding for Detection and Defense of Sink Holes in Wireless Reconfigurable Networks, IEEE ICSNC, 2008.

[7] Villalpando, R., Vargas, C., Munoz, D., Interference and Outage evaluation of a Network Coding based Detection and Defense Mechanism for WRN, 2009 Third International Conference on Digital Society.

[8] Ji-Yong P., Ryu M. S., Suk J. E., Dong-Min S., Park H. S., An Integrated Security Mechanism for Network Coding Combining Confidentiality in ICACT 2009, pp. 311-314.

[9] Soo-Kim, N., Beongku, A., Do-Hyeon, K., Ye Hoon, L., Wireless Ad-hoc Networks Using Cooperative Diversity-based Routing in Fading Channel, Communications, Computer and Signal Processing, 2007, pp. 70-73.

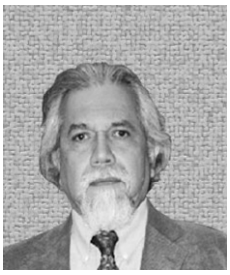
Authors´ Biographies

Rafaela VILLALPANDO-HERNÁNDEZ

She received her Ph.D. in electronics and telecommunications engineering from Instituto Tecnológico y de Estudios Superiores de Monterrey (Technological Institute of Higher Education of Monterrey), ITESM, Campus Monterrey, in December 2008. Thereafter, she joined the Engineering Center at the ITESM, Campus Laguna, Torreon, Mexico. She has participated in several research projects involving network coding, position location in wireless networks and implementation of sensor networks. Her research interests include wireless and sensor networks.

Cesar VARGAS-ROSALES

He received a Ph.D. in electrical engineering from Louisiana State University in 1996. Thereafter, he joined the Center for Electronics and Telecommunications at Instituto Tecnológico y de Estudios Superiores de MonterreyMonterrey (, ITESM), Campus Monterrey, Mexico. Dr. Vargas has been ais member of the National System of Researchers (Sistema Nacional de Investigadores), (SNI,) since 1997, and is the coauthor of the book Position Location Techniques and Applications. He has carried out research in the area of personal communication systems on CDMA, smart antennas, adaptive resource sharing, location information processing, and multimedia services. He was a Technical Program Chair for IEEE Wireless Communications and Networking 2011. His research interests are personal communications networks, position location, mobility and traffic modeling, intrusion detection, and routing in reconfigurable networks. Dr. Vargas is the IEEE Communications Society Monterrey Chapter Head and has been a Senior Member of the IEEE since 2001.



David MUÑOZ-RODRIGUEZ

He received a B.S. degree in 1972, an M.S. degree in 1976, and a Ph.D. degree in 1979 in electrical engineering from the Universidad de Guadalajara (University of Guadalajara), México, Cinvestav, Meéxico, and University of Essex, Colchester, England, respectively. He is Senior Member of the IEEE and was formerly Chairman of the Communication Department and Electrical Engineering Department at Cinvestav, IPN. In 1992, he joined the Instituto Tecnológico y de Estudios Superiores de Monterrey, ITESM), Campus Monterrey, Meéxico, where he became the Director of the Center for Electronics y Telecommunications. His research interests include wireless systems and performance analysis.

Jose RAMON-RODRIGUEZ

He received his Ph.D. in electrical engineering from CINVESTAV-IPN Zacatenco in August 2000. Thereafter, he joined the Center for Electronics and Telecommunications at Instituto Tecnológico y de Estudios Superiores de Monterrey, ITESM, Campus Monterrey, Mexico. He was a member of SNI for 8 years. He participated in several Government projects involving security and RF systems implementation.