Stochastic Modeling of Hello Flooding in Slotted CSMA/CA Wireless Sensor Networks

Mohammad Sayad Haghighi, Kamal Mohamedpour, Vijay Varadharajan, and Barry G. Quinn †

Abstract— Broadcasting a request or challenge is a classic method of collecting local information in distributed wireless networks. Neighbor discovery is known to be a fundamental element in ad hoc and sensor networks topology formation, which takes advantage of such methods. Most of the current neighbor discovery protocols rely on a challenge or request broadcast by the discovering node called “Hello”. Hello flooding attack was specifically designed to exploit the broadcasting nature of these protocols in order to convince a large group of nodes that the sender is their neighbor by using very high transmission power. Several studies have been done to mitigate the effectiveness of the flooding threats but little effort has been made in modeling and analyzing this problem. Arguing that random channel access protocols must be inevitably employed in neighbor discovery, we propose an analytical approach for stochastic modeling of the challenge-broadcasting scenarios in slotted CSMA/CA wireless sensor networks. We model the non-stationary channel right after issuance of the request by a recursive method and then put forward an approach to find the broadcaster’s approximate payoff. The model also supports the cases where the broadcaster is a malicious node with an abnormally high transmission and reception range, which is found in severe flooding attacks. We investigate the applications of the model in finding the optimal attack range for the flooding adversaries and deriving a flood-resilient MAC protocol design framework to increase the security of challenge-response protocols. The latter one is especially relevant to mobile networks as it provides a low cost solution. This paper describes the detailed analysis of the proposed theoretical framework as well as the comprehensive evaluations that have been carried out via simulations.

Index Terms— Hello Flooding Attack, Sensor Networks, Carrier Sense Multiple Access (CSMA)

I. INTRODUCTION

Wireless sensor networks, as a subset of ad hoc networks, are spontaneous systems that consist of several similar nodes which are devoid of any coordinator and are usually employed for monitoring purposes. These networks have variety of applications ranging from fire alarm systems in the forests to enemy movement detection systems in the battlefield [1].

Security in sensor networks has always been a challenging issue since their conception. The infrastructure-less nature of the architecture along with the wireless connectivity, multi-hop transmission, and low energy and processing power give rise to a range of security threats and vulnerabilities [2]. The special characteristics of sensor networks have let new forms of threats emerge which are specific to these networks. In addition to the previously known sleep deprivation attack, Karlof and Wagner [3] introduced a new effective attack for sensor networks called Hello flooding which exploits the broadcasting nature of neighbor discovery protocols.

Broadcasting a challenge or request is a very common way of data collection or data dissemination. For example, in sensor networks, a cluster head may issue a request through broadcasting to collect all the sensed values in its vicinity [4]. In neighbor discovery, as another example, every node broadcasts a request or challenge (Hello) which includes its identity (and potentially mutual cryptographic key constructing parts). In one-way protocols, the receivers add the sender’s ID to their neighbors list after processing the message. In two or multi-way protocols the sender is able to identify its neighbors through processing the incoming responses.

In the Hello flooding attack, Hello message is advertised with a very high-power. This may convince many surrounding nodes that the malicious transmitter is one of their neighbors. Several works have been done to counteract this threat [3, 5-19], but little effort has been made in modeling it. Any protocol which relies on broadcast information to fulfill its tasks may be vulnerable to flooding attacks. If the modeling leads to the development of a countermeasure for the Hello flooding attack, it can also be useful in securing other broadcast-based protocols.

The necessity of using a two or multi-way protocol for neighbor discovery has been addressed previously with respect to the security constraints [3, 20, 21]. In a two-way protocol, when a node broadcasts a request, each receiving node tries to send an appropriate reply packet back. The replying nodes’ medium access control (MAC) layers have to capture the common channel one at a time in order to transmit their data. In the absence of transmission-scheduling coordinators in infrastructure-less networks like sensor networks, random channel access protocols are the only candidates for the MAC layer. Besides in the neighbor discovery case, there exists no prior information about the network graph while running the protocol. Any scheduled type of transmission, including the time division multiple access methods, implies the existence

† Manuscript received October 29, 2010; accepted July 12, 2011. M. Sayad Haghighi (corresponding author) and K. Mohamedpour are with the Department of Electrical Engineering, K. N. Toosi University of Technology, Tehran, Iran (e-mail: sayad@ee.kntu.ac.ir, kmpour@kntu.ac.ir).
V. Varadharajan is with the Department of Computing, Faculty of Science, Macquarie University, Sydney, NSW, 2109, Australia (e-mail: vijay.varadharajan@mq.edu.au)
B. G. Quinn is with the Department of Statistics, Macquarie University, Sydney, NSW, 2109, Australia (e-mail: bquinn@efs.mq.edu.au).
of a table for transmission times and number of nodes sharing the channel which cannot be provided prior to neighbor discovery.

A benign data collection or aggregation scenario can be usually studied under the single-cell network assumption; this is not possible for a flooding scenario. In single-cell networks, every node can receive every other node’s transmissions. But in the Hello flooding attack, the malicious node’s broadcast range is so high that the responders may not be in radio proximity of each other and cannot sense each other’s transmissions and hence, form a non-single-cell network.

In this article, we address analytical modeling of unacknowledged slotted CSMA/CA-based broadcasting challenge-response protocols in sensor networks. The modeling procedure is split into two parts. First, a non-stationary model of the after-broadcast channel is developed. In the channel modeling approach, we have taken the flooding attacks’ specifications into account, i.e. the situations where the transmission range of the broadcaster is significantly larger than the benign operation range. Second, using the model developed in the first part, a method is presented to estimate the broadcaster’s payoff. In the Hello flooding attack, this payoff would be the number of neighbors the adversary will have after fulfilling the protocol but deviating from the regular transmission power rules.

This paper is organized as follows: In Section II, a summary of the related studies is presented. In Section III, a recursive method is proposed to model the channel non-stationary behavior after issuance of the challenge. Section IV introduces a method to approximate the broadcaster’s payoff. The simulation results are given in Section V. Section VI describes some of the applications of the model and finally the conclusion is given in Section VII.

II. RELATED WORK

At a high level, the data collection and Hello flooding problems, can both be considered as translations of the broadcasting challenge-response problem and the only difference is in the range of the broadcast. Of the previous studies in this area, a few authors have tried to model the data-collection scenarios, however none of them are general enough to support for the flooding scenarios too. Our proposed model is general in the sense that it supports both benign and flooding scenarios. Therefore, we will review the studies on the Hello flooding attack as well as the data-collection problem with an emphasis on the theoretical models.

Karlof and Wagner [3] were the first who noticed a flooding threat in sensor networks while studying the neighbor discovery problem. They called it Hello flooding attack. In one-way neighbor discovery protocols, when a Hello message is broadcast, the receiving nodes add the sender’s ID to their neighbors list. A node-compromising (internal) adversary can exploit the broadcasting nature of this protocol to convince numerous nodes that it is their neighbor through transmission of Hello packet with very high power. The authors themselves proposed verifying bi-directionality of the links as a means to counteract flooding attacks and this implicitly means use of a two or multi-way challenge-response protocol. But this solution becomes useless when the adversary is equipped with a sensitive receiver i.e. a receiver with high reception range.

Then papers addressing this problem appeared. A group of papers proposed power-based solutions. Inspired by the study done by Zhen et al. [6], Singh et al. [7] proposed a countermeasure for the Hello flooding attack based on signal strength measurements and client puzzles. In this approach, the nodes are classified into “friend” and “stranger” groups, according to the signal power measurements. Requests with very abnormal powers are rejected. The strangers are then asked to solve puzzles. Aside from the puzzles which incur computational cost and are only useful if the number of requests is high, the received power level is not a good index to rely on for protection purposes. Korkmaz [9] has formally shown that power-based countermeasures can be thwarted by colluding attackers.

Estimating the distance is another way of finding fraudulent neighborhood claims. For non-compromising (external) attacks, Brands et al. [22] were the pioneers of using this method with their one-bit exchange protocol. The distance bounding method they proposed was a cryptographic protocol that could put an upper bound on the distance between two nodes. Their protocol was later shown to be vulnerable to internal attacks [23]. Based on the same initial concepts of distance bounding, Sastry et al. [8] proposed a similar protocol named “Echo protocol”. Hu et al. [24] also introduced two methods to localize the claiming nodes; temporal leashes and geographical leashes. The former one is an adoption of the same idea of distance estimation based on the signal travel time. The sender is supposed to add a timestamp to the packet before transmission. In the latter method, the sender also sends its geographical location. Based on this information, the receiving node investigates the validity of the request origin. Korkmaz [9] addressed the signal round trip time measurement in the presence of adversaries on a separate channel in which the signal propagation speed is faster than the medium normal nodes operate on. The author derived a hard threshold to decide on the legitimacy of the requesting node’s distance. In a combined work of distance measurement and graph abnormality detection, Shokri et al. [5] suggested each node to be equipped with two transceivers; one Radio Frequency (RF) and one Ultra Sonic (US). The RF transceiver is used for clock synchronization purposes while the US transceiver is used for precise distance measurements. This solution is accompanied by a distributed graph abnormality detection technique. However, this work suffers from some flaws in the preliminary assumptions [21].

Poturalski et al. [20, 25] classified neighbor discovery protocols into time-based and time-and-location-based groups and wrote them in a general formal manner. Putting an end to the time-based efforts, the authors proved that it is impossible for the protocols which solely rely on signal propagation time measurements to provide seamless security. However, time-and-location-based protocols were shown to be able to secure neighbor discovery against external attacks. The authors later divided the neighbor discovery protocols into beacon-based and challenge/response-based sub-groups and formally derived the set of conditions under which each of these can be secure against external attacks [25].

Aside from the classic power-based, time-based and time-and-location-based solutions, there are some other heuristic
studies addressing the Hello flooding attack. Using a probabilistic approach, Khozium [10] suggested that a set of randomly selected nodes receiving Hello request report it to the sink so that the sink validates the legitimacy of the request. This method is not scalable and is conceptually equivalent to the centralized graph abnormality detection methods [26].

Using a challenge-response protocol, [11] and [12] proposed that the nodes initially verify local neighbors and establish pairwise keys based on the set of common keys derived from a tree of shared secrets. Each broadcast request is supposed to be encrypted with a key generated on the fly. This way, any node’s reachable neighbor can decrypt and verify the broadcast message while the external attackers cannot. Accepting the deficiency of this method in facing internal compromising adversaries equipped with sensitive receivers, the authors proposed a multi-path multi-base station data forwarding alternative to improve the data delivery and integrity.

So far, we have gone through the papers which addressed the flooding problem facing non-compromising adversaries. In compromising (internal) attacks, since one side of the protocol which sends legitimate messages is malicious itself, it is impossible to rely on either time or location information provided by the other party. To solve this problem, some authors tried to limit the nodes’ communication range by cryptography. In the majority of these methods it is assumed that compromising a node takes a certain amount of time \(T_{\text{min}}\). So it is suggested that mutual keys are established during this period, right after the network deployment. Secure Cell Relay (SCR) routing protocol [13, 14] uses a three-way challenge-response mechanism to avoid unidirectional-link-oriented problems facing the Hello flooding attack. A master key is used to establish the mutual keys. The master key is deleted from the nodes’ memory before \(T_{\text{min}}\) elapses from the deployment. Since each node is bound to communicate only with the nodes with which it has initially established keys, supporting mobility is impossible in this framework. LEAP and later LEAP+ [15, 16] were two cryptographic methods which followed the same principles as SCR. However, unlike the SCR protocol, they did not use any timestamps. The authors claim that these methods are able to counteract Hello flooding. In [21] the authors have challenged this claim putting forward an attack which can create a Hello flood in two steps. Saghar [17] used the same principle of establishing mutual keys in the after-deployment immune time interval. This study is accompanied by a formal investigation of security using model checking software. The Hello flooding attack has been modeled by modifying the nodes’ connection matrix to represent the fact that the attacker can establish unidirectional links. This implies that the author has assumed adversaries with insensitive receivers. In [18], taking a similar approach, the authors proposed a data collection protocol. Hello flooding attack is claimed to be thwarted by the initially established local mutual keys. The authors used AVISPA tool [27] to formally verify their protocol security. All of these studies have the same mobility issues as SCR.

In [21], taking a different approach from those who used cryptographic solutions, we defined the notion of statistical security against broadcast-type attacks. In a taxonomy of reactions to flooding, we defined three distinct profiles of network behavior; insecure, robust and secure. In the robust profile, the gain of the attacker is higher than the benign case but still limited. In [19], a statistical countermeasure of robust type has been evaluated by means of simulation against flooding adversaries equipped with sensitive receivers. The association procedure of the MAC layer of the IEEE 802.15.4 standard was manipulated with the aim of embedding the concept of link bi-directionality test. However, the focus is mainly on the timing of reply packets arrival. Unlike the cryptographic solutions, statistical countermeasures can be used in mobile networks and incur low cost.

Hello flooding attack targets neighbor discovery service which is usually implemented in the MAC layer. A theoretical model can come to work both in neighbor discovery protocol parameters optimization for the benign scenarios and development of more effective statistical countermeasures in the malicious ones. Although no effort has been made in modeling the flooding scenarios, there have been some studies on the benign ones in data-collection and aggregation-related papers. Due to the existence of a time synchronization point (the beacon or challenge in our terminology), most of the studies in this area have focused on the slotted medium access control protocols.

In a slotted CSMA/CA-based data-collection scenario, Leibnitz et al. [4] tried to model the IEEE 802.15.4 MAC layer behavior for a cluster of nodes which start their contentions simultaneously. To model the transient response of the system to the challenge, the authors used a Markov chain to locate the global system state as the time goes by. However, their analysis is valid only in single-cell scenarios and besides, they have assumed a fixed channel busyness probability which is an unrealistic assumption [28]. Since each node transmits only once, the number of contenders reduces as the time passes. This leads to the gradual decrease of the channel busyness probability. Shu et al. [29], studied a similar problem with a different approach but still using a Markov model to follow the general state of the single-cell IEEE 802.15.4-based network. The authors assumed that the nodes start their contention simultaneously in order to transmit without acknowledgments. They defined each state based on three variables; namely, the number of backoff nodes, the number of timeslots that have been used for the ongoing transmission(s) and the number of nodes which have successfully captured the channel with no collision till each timeslot. In [30], the authors pursued the same approach as Shu et al., but they modified the previous Markov model and added one more dimension to it defining each state with four variables in order to mitigate the flaws it had.

In this paper, we analytically model the unacknowledged slotted CSMA/CA-based broadcasting challenge-response protocols which also covers non-single-cell scenarios i.e. the scenarios in which the nodes are not necessarily in radio proximity of each other. Such a condition has not been studied in any of the above-mentioned papers. Furthermore, in Hello flooding attacks whose study is one of the main goals of this model development, the number of nodes being addressed may count up to thousands. The majority of the models presented use the power method to follow the network state over time [4, 29, 30]. Even if they could be extended to support for non-single-cell scenarios, the matrices dimensions
would dramatically increase making them practically impossible to employ.

In the next section we analyze the after-broadcast channel for slotted CSMA/CA-based protocols. The results obtained are then used in the following section to find the broadcaster’s mean payoff both in benign and malicious scenarios.

III. STOCHASTIC MODELING OF THE NON-STATIONARY CHANNEL IN SLOTTED CSMA/CA-BASED BROADCASTING CHALLENGE RESPONSE PROTOCOLS

Assume that a request has been broadcast in a uniform network and the receiving nodes are expected to respond to it with small information-carrying packets of fixed length. The channel is common. Hence, the nodes have to follow a channel accessing protocol to compete in capturing the channel. This contention is done locally among the nodes which are in the carrier sense range of each other. At this point, for simplicity, let us assume that the dimensions of the active area are infinite and that we want to statistically model an arbitrary node’s transmission behavior. From physics point of view, the network can be thought of as a set of particles locally interacting with each other. An event affects all the particles at the same time and they react to this stimulant. Since they all have similar characteristics, if somebody investigates any of the particles behavior, it will be statistically similar to the others’ as each of those particles is surrounded by a set of similar particles which are exactly following the same rules to react to the stimulant. This notion is called Mean Field Theory (MFT) and the main idea of MFT is to replace all the interactions effect to any member of the system with an average or effective interaction. This reduces a multi-body problem to an effective one-body problem. Through solving an MFT problem, we can gain insight into the behavior of the system at a relatively low cost. In this paper, we apply the MFT notion to the broadcast attack scenarios. In our case, the perturbation is expected to subside after a while since the nodes gradually either transmit their packets or fail as the time passes.

Assume an arbitrary node is trying to capture the channel following slotted CSMA/CA protocol in order to send its reply packet. A Markov model of such protocol adopted from the IEEE 802.15.4 standard [31] is depicted in Fig. 1. The only difference is that its contention window size (CW) is one (uses one Clear Channel Assessment (CCA)) while IEEE 802.15.4 uses a window size of two. When the MAC layer has a packet to transmit, it first backs off for random number of timeslots chosen from the interval \([1,2^{BE_{min}}]\), where \(BE_{min}\) is the minimum backoff exponent. Then, it senses the channel in the CCA state and if the channel is free, it starts transmitting in the minimum backoff exponent. If the MAC layer cannot find the channel free after \(NB_{max}\) backoffs, it gives up contending for the channel and reports a failure to the upper layer. Each time the channel is sensed in the CCA states, the nodes’ models become dependent. However, with MFT notion, we can substitute all of those nodes’ effects with an equivalent channel busyness probability and decouple the models.

Since we are dealing with a transient time-limited event, unlike many other papers which are mainly inspired by Bianchi’s approach to model steady-state channels [32], we cannot use a fixed channel busyness probability. Moreover, as each node replies to the request only once, we have a special non-saturated non-stationary case to model. Here, from an arbitrary node’s point of view, the channel busyness is a non-stationary random process and to describe it, we have to have its characteristics over time. To a node, the channel status in each timeslot can be either busy or free. A Bernoulli random variable can well describe the channel busyness probability in a timeslot. We define \(P_b(t)\) to be the probability of the channel being busy in the \(t^{th}\) timeslot from an arbitrary node’s point of view. If we obtain the effective \(P_b(t)\) based on the real scenario where distributed spatial correlation exists among the nodes’ transmissions, then we can use this effective \(P_b(t)\) in each node’s Markov model assuming that they are decoupled and approximate the same real-world statistics for transmissions.

Let us denote the number of timeslots a node waits in the \(k^{th}\) binary exponential backoff by \(B_k\) which is a uniform random variable over the interval \([1,W_k]\) where \(W_k = 2^{min\{BE_{min}+k,BE_{max}\}}\); \(0 \leq k \leq NB_{max}\). We define \(b_k(t)\) as the probability of the event \(\{B_k = t\}\):

\[
b_k(t) = P(B_k = t) = \begin{cases} \frac{1}{W_k} & 1 \leq t \leq W_k \\ 0 & \text{oth.} \end{cases}
\]
Based on the above explanation, we define $d_k(t)$ to be the probability that a node reaches CCA state at timeslot $t$ ($t \geq 1$) after $k$ backoffs. The recursive form of $d_k(t)$ is given in Eq. (3).

$$d_k(t) = \sum_{t_k=t}^{t-1} \left( \sum_{t_{k-1}=t}^{t-1} \left( \sum_{t_{k-2}=t}^{t-1} \ldots \sum_{t_{1}=t}^{t-1} b_0(t_0) P_b(t_0)b_1(t_1-t_0) \right) \right) \ldots P_b(t_{k-1})b_{k-1}(t - t_{k-1})$$

\hspace{1cm} (2)

$$d_k(t) = \sum_{t_{k-1}=t}^{t-1} \ldots \sum_{t_{1}=t}^{t-1} b_0(t) \quad k = 0$$

\hspace{1cm} (3)

where $d_k(t) = 0$ for $t \leq k$. Having $P_b(\tau)$ for $\tau = 1, \ldots, t-1$, $d_k(t)$ can be easily computed. $d_k(t')$; $t' = 1, \ldots, t$ and $P_b(t'')$; $t'' = 1, \ldots, t$, in turn can be used for the calculation of $P_b(t + 1)$. The recursive nature of these equations helps us use each timeslot busy probability as a building block for the next timeslots. $P_b(1) = 0$ can be used as the initial condition since even if a node’s timer expires at $t = 1$, the transmission cannot be started till the next timeslot. For the CSMA/CA model at hand, Eq. (4) gives the probability of transmission at time $t$.

$$P_t(t) = \sum_{k=0}^{NB_{\text{max}}} d_k(t-1). (1 - P_b(t-1)) \quad t > 1$$

(4)

It is clear that $P_1(1) = 0$ since there exists no timeslot for a CCA prior to $t = 1$. Assume that there are $N$ nodes around the broadcaster who are contending to send packets of length $L$ over the channel. The transmitting nodes are not necessarily in each other’s carrier sense range so we may have simultaneous or overlapping transmissions in different regions of the affected area. This phenomenon is similar to the so called hidden node effect [33]. The busy channel probability in the $t$th timeslot depends on the tails of the packets transmitted at most $L - 1$ slots ahead in time. We call each combination of these probable transmissions a “state”. Fig. 2 shows a sample state which affects the busyness of the channel in the $t$th timeslot directly when $L = 4$. The demonstrated state is composed of four transmissions; one at $t - 3$, two at $t - 2$ and one at $t$. Notice that the analysis window is $[t - L + 1, t]$. Obviously there is a dependency between the transmissions of overlapping packets since each ongoing transmission temporally reduces the area in which the channel is free. If we trace this dependency it goes back to slot one as the probability of every transmission at $t$ depends on the possible transmission events in the interval $[t - L + 1, t - 1]$ and those events, in turn, are chained to the previous set of events. To avoid falling into the complexity of such analysis we do a precise temporal analysis in the interval which affects the busyness of the channel in the $t$th timeslot directly, but we use the average effect of all the states in the past timeslots reflected in $P_b(t)$. In Fig. 2, this non-stationary effective channel behavior model in the interval $[1, t - 4]$ is shown with a cloud to which the nodes’ backoff timers point and from which some that sensed the channel busy come out. Someone sitting outside the system can find the total number of states using Eq. (5).

$$N_{\text{states}} = \frac{(L + 1)(L + 2) \ldots (L + N)}{N!}$$

(5)

However, in the temporal analysis, since we intend to model the channel a node experiences in the presence of other nodes, we have to substitute $N - 1$ for $N$ in the above equation i.e. in the temporal analysis we aim finding $P_b(t)$ from an arbitrary node’s point of view which has not contributed to the channel busyness yet. As we explain later, many of these states have small or zero probability of occurrence and many others will result in the channel busy probability being one in their $L$th slot. We denote the set of all such states by $\Omega_e$. Since the states are mutually exclusive we can write:

$$P_b(t) = \sum_{i \in \Omega} P_b(t \mid S_i) \cdot P(S_i)$$

\hspace{1cm} (6)

$$\approx 1 + \sum_{i \in \Omega_e} (P_b(t \mid S_i) - 1) \cdot P(S_i)$$

where $S_i$ is the $i$th state at time $t$ and $\Omega$ and $\Omega_e$ are the sets of all possible, and reduced states respectively. A state is a combination of overlapping and simultaneous transmissions. We shall find the probability of occurrence of these transmissions in a $L$-slot window ending at time $t$ for $P(S_i)$, and how much each combination makes the common channel busy, for $P_b(t \mid S_i)$. The conditional probability term value does not depend on $t$ (refer to Fig. 2). We focus on the conditional probability term calculation first and then derive a recursive method to obtain $P(S_i)$.

In a challenge-broadcasting scenario like the flooding one, the requesting node advertises a message up to the radius $R$. The receivers are expected to reply with small information-carrying packets. We assume we are dealing with homogenous sensor networks and the nodes have equal transmission power. Each transmitting node temporally makes its surrounding area busy in radius $r_c$ which is the carrier sense range and is greater than the reception range $r_e$ in practical scenarios.

According to the CCA mechanism, in any state, transmitters of a specific timeslot (simultaneous transmissions) can be located geometrically anywhere in the non-busy area while transmitters of different timeslots (overlapping transmissions) should be apart from each other by the distance $r_c$. Depending on the ratio $\eta = \frac{r_c}{R}$, only a limited number of overlapping transmissions can exist i.e. a limited number of such transmissions which are not in the carrier sense range of each
other are able to carpet the whole area affected by the broadcaster. We denote this number by \( N_c \). Since the graph must be connected and \( r_a \geq r_x \), the condition \( N \geq N_c \) usually holds. \( N_c \) solely relies on the \( \eta \) value and once it is calculated, it can be reused for other configurations with different values of \( r_a \) and \( R \) (see Appendix I, Theorem 1). Fig. 3 shows the mean busy channel assessment probabilities versus the number of overlapping transmissions derived from Eq. (20). When \( \eta \) is large, a small number of transmissions make the channel busy all over the area affected by the adversary. When it gets smaller, e.g. when the attack range is significantly larger than the benign carrier sense range, more (overlapping) transmissions are required to make the medium completely busy and thus, the curves show moderate rises with lower slopes. In each case, the value of \( N_c \) is where the curve intersects the horizontal line \( P_b = 1 \). If \( L > N_c \), then all the states with more than \( N_c \) transmissions in different timeslots will have zero probability of occurrence. This constraint can significantly reduce the size of \( \Omega_e \), especially when \( \eta \) is large. For \( \eta \geq 2 \) (a condition met in single-cell scenarios), \( N_c = 1 \).

Similarly, states with high number of simultaneous transmissions can result in a busy channel probability of one.

The number of simultaneous transmissions causing a certain level of busyness depends only on the \( \eta \) value (Appendix I, Theorem 2). Fig. 4 shows the busy channel probability versus the number of simultaneous transmissions derived from Eq. (26). One can limit the maximum number of simultaneous transmission to a value like \( N_e \) by approximation to further reduce the size of \( \Omega_e \) set. Generally, a state is composed of both overlapping and simultaneous transmissions. Although this means the actual \( \Omega_e \) set is much smaller than what is defined solely based on \( N_c \) or \( N_e \), finding the combinations which lead to the busy channel probability of one (or close to one by approximation) in the \( L^\text{th} \) slot is not a trivial task. But, since to achieve a certain level of busyness \( N_e \geq N_c \), one can find an upper-bound for the number of \( \Omega_e \) members by substituting \( N_e \) for \( N \) in Eq. (5).

The conditional probability term values for the set of \( \Omega_e \) members solely depend on \( \eta \) and can be calculated once for different \( \eta \) values and be reused in other design configurations. With the upper bound given on the \( \Omega_e \) size before, one can also put an upper bound for the number of conditional probability calculations required as:

\[
N_f = \sum_{n=1}^{N_f} \sum_{k=1}^{L} \left| \frac{n_s^k}{k} \right|
\]

where \( \frac{a}{b} \) stands for the number of ways \( a \) can be partitioned into \( b \) parts, that is equivalent to the number of different distributions of \( a \) indistinguishable balls among \( b \) indistinguishable bins so that no bin is left empty. From the definition it is obvious that \( \frac{a}{b} = 0 \) if \( b > a \).

In order to obtain \( P(S_f^i) \) value, we have to represent \( S_f^i \) in the form of the intersection of slot-based events as \( s_f^i \cap s_f^2 \cdots \cap s_f^L \). When \( \sum_{u=1}^{L} n_s^i u + 1 \), \( P(S_f^i) \) can be found using Eq. (8).

\[
P(S_f^i) = P\left(s_f^1 \cap s_f^2 \cdots \cap s_f^L\right)
= P\left(s_f^1\right) \times \prod_{j=1}^{L-1} P\left(s_f^{i+j+1} \cap s_f^1 \cap \cdots \cap s_f^{i+j}\right)
\approx \left(\frac{N-1}{n_s^1}\right)^{n_s^1} \left(P_t(t-L+1)^{n_s^1} \left(1-P_t(t-L+1)\right)^{N-n_s^1}\right)^{n_s^1-1}
\times \prod_{j=1}^{L-1} \left(\frac{N-\sum_{u=1}^{j} n_s^i u - 1}{n_s^i j+1}\right)^{n_s^i j+1} \left(P_t(t-L+j+1)^{n_s^i j+1} \left(1-P_t(t-L+j+1)\right)^{N-n_s^i j+1}\right)^{n_s^i j+1-1}
\]

1 The general table of busy channel probabilities for efficient states with different \( \eta \) values and the tree of conditional probabilities of the payoff analysis have already been computed and stored in a lookup table.

2 There exists no simple closed-form formula for counting the number of different distributions of \( a \) indistinguishable balls among \( b \) indistinguishable bins with the constraint that no bins are left empty. However one can take advantage of the following recursion: \( \frac{\binom{n}{r}}{r!} = \frac{\binom{n-r}{r-1}}{(r-1)!} + \frac{\binom{n-1}{r-1}}{(r-1)!} \).
In order to compute events \( \{ s_t, \ldots, s_t \} \), we may write:

\[
P_t(t) = \prod_{j=0}^{NB_{\text{max}}} d_k(t) \prod_{j=0}^{NB_{\text{max}}} d_k(t)
\]

The interesting point about this equation is the movement of the terms backward in time with respect to the initial time \( t - j + 1 \). According to Eq. (3), \( d_k(t) \) is itself constructed by \( P_b(t) \) and \( d_k(t) \) for \( 1 \leq t \leq j \). After moving backward for \( j \) slots, the conditions disappear and we may use the effective probability over all such states. This algorithm reduces a complex problem to a simple selection and (weighted) probability over all such states. This algorithm reduces a complex problem to a simple selection and (weighted) probability over all such states.

Fig. 5 using dotted lines. The conditional probability at one transmission at \( t \) and the transmissions are separate. In the former case, no overlapping transmissions are possible. In the latter case, the Signal to Interference Ratio (SIR) in all timeslots however the state probabilities are not; finally, the numerator computes \( P_b(t - 3) \).

Now we have enough information to start a recursive procedure to derive \( P_b(t) \) using Eq. (6). One can also use the result obtained to find other valuable quantities such as the mean delay, the mean transmission failures or their distributions over time. In Section V, we validate the theory developed in the previous section and show that the theoretical model well predicts the practically found \( P_b(t) \) curve.

### IV. BROADCASTER’S PAYOFF ANALYSIS

The broadcaster’s payoff is defined to be the number of decodable reply packets. The quantities that affect the payoff are the number of transmitters and the probability density functions (pdf) of their distances to the broadcaster in each timeslot. Assume a uniformly deployed set of sensors with the density \( \delta \). We make an approximation by assuming that with the ever-decreasing number of contending nodes, at any time, the remaining nodes will still have the uniform distribution. This approximation is errorless under \( R \gg r_c \) or \( R \leq r_c/2 \) condition. If we denote the distance of a node inside the affected area to the broadcaster by \( r \), then the pdf of \( r \) will be:

\[
f_r(r) = \frac{2r}{R^2}; \quad 0 \leq r \leq R
\]

where \( R \) is the broadcast range. Here we make some assumptions to avoid any ambiguities may arise later. The distances of two (or more) nodes whose packets directly or indirectly overlap might be dependent. However, this dependency can be ignored when \( R \leq r_c/2 \) or when \( R \gg r_c \) and the transmissions are sparse. In the former case, no overlapping transmissions are possible. In the latter case, the network dimensions are so large that a single transmission does not make a noticeable area of the network busy and hence, the independence assumption holds with high probability.

For the broadcaster to be able to decode a packet correctly, the Signal to Interference Ratio (SIR) in all \( L \) slots must be greater than a theoretically-derived threshold for errorless reception which we will denote by \( T_r \). This threshold depends on the physical layer specifications and the modulation method employed. A packet is presumed to be lost or corrupted if it is not decodable in at least one slot. Notice that when two (or more) packets are either sent simultaneously or overlapping in time, an adversary might still be able to decode corrupted if it is not decodable in at least one slot. Notice that when two (or more) packets are either sent simultaneously or overlapping in time, an adversary might still be able to decode corrupted if it is not decodable in at least one slot.

\[
f_r(r) = \frac{2r}{R^2}; \quad 0 \leq r \leq R
\]
We assume having a cross-layer laptop-class adversary \([3]\) whose receiver is sensitive enough to demodulate the packets sent from nodes as far as distance \(R_r > r_{tx}\). We know that \(R > r_{tx}\). If \(R_r < R\), then there will be interferences from the replying nodes residing in the ring characterized by \(R_r < r \leq R\) over the ones located inside the circle \(r \leq R_r\). To find the upper bound for the adversary’s payoff, we analyze the worst case scenario i.e. \(R_r = R\). Moreover, the received signal is always accompanied by the thermal noise. Since we assumed that the adversary can receive the signals sent from the farthest nodes in its range, even the weakest signals are powerful enough to suppress the thermal noise factor. Therefore, in the calculations the thermal noise contribution can be ignored with respect to the power of other interfering transmissions.

Fig. 6 demonstrates a sample of overlapping packets (states) at the broadcaster’s receiver causing interference for decoding of a packet sent at time \(t\). The states are \(2L - 1\) slots long.

Let \(\psi_i\) be the event that the \(i^{th}\) node’s packet (which we call the tagged node’s packet from here on), is successfully received by the broadcaster. The indicator random variable \(Y_i\) is defined by Eq. (12).

\[
Y_i = \begin{cases} 
1 & \text{if } \psi_i \\
0 & \text{otherwise}
\end{cases}
\tag{12}
\]

Although \(Y_i\) and \(Y_j\) \((i \neq j)\) are not independent, due to the linear properties of the expectation operator, one can find the adversary’s mean payoff \(S_a\) through the following:

\[
S_a = E \left[ \sum_{i=1}^{N} Y_i \right] = \sum_{i=1}^{N} E[Y_i] = N \cdot P[\psi_i]
\]

\[
= N \cdot \left( \sum_{i=1}^{t_{max}} P[\psi_i | \theta_i] \cdot P[\theta_i] \right) \approx N \cdot \sum_{i=1}^{t_{max}} P[\psi_i | \theta_i] \cdot P(t)
\]

\[
= N \cdot \sum_{i=1}^{t_{max}} P(t) \sum_{j \in U_i} P[\psi_i | \theta_i] \cdot P(S_i | \theta_i)
\]

\[
\approx N \cdot \sum_{i=1}^{t_{max}} P(t) \left( P(s_i | \theta_i) \times \prod_{k=1}^{L-1} P(s_i | \theta_i) \right)
\]

And adding the necessary condition \(N \gg \sum_{i=1}^{L-1} n_{s_i} + 1\), we may write:

\[
S_a \approx N \sum_{t=1}^{t_{max}} P(t) \sum_{j \in U_i} P[\psi_i | \theta_i] \cdot P(S_i | \theta_i)
\]

\[
\times \left( (N - 1) \left( n_{s_i} \right) \cdot P(t) \cdot (L - 1) \right)^{n_{s_i} - 1}
\]

\[
\times \prod_{k=1}^{L-1} P(s_i | \theta_i) \times \prod_{k=1}^{L-2} P(s_i | \theta_i)
\]

\[
\]
we can rewrite Eq. (15) as below:

\[ \bigcup_{k=1}^{z-1} \{ \phi_{e_k}^k > T_r \} \cap \{ \theta_i^j \cap S_i^j \} \]

\( \phi_i^h \) and \( \phi_i^j \) (\( h \neq j \)) are not independent. The number of intersection operations in Eq. (15) can be usually reduced since for many states, the events \( \{ \phi_i^1 > T_r \}, \ldots, \{ \phi_i^L > T_r \} \) are highly dependent. For instance, in Fig. 6, if the SIR is higher than \( T_r \) at \( t + 1 \), then it will be higher than this threshold at \( t + 2 \) too. Starting from \( t - L + 1 \) (corresponding to the event \( \{ \phi_i^1 > T_r \} \)), depending on the state, if the interfering transmitters either stay the same or are solely added or reduced in each slot with respect to the previous one when we move forward in time, the intersection operator eliminates one of the redundant events with each move. After this simplification, there will remain partially dependent events \( \{ \phi_{e_k}^k > T_r \}, \ldots, \{ \phi_{e_z}^z > T_r \} \) where \( z \leq L \). Using the chain rule we can rewrite Eq. (15) as below:

\[ P(\psi_i^h \cap S_i^j) = P(\psi_i^h > T_r) \cap (\theta_i^j \cap S_i^j) \]

Excluding the first term, computation of the above conditional probabilities requires multi-dimensional integrations with complex bounds. However, as both the events and conditions have random variables appearing in the form of rational numbers, the value of these integrals will be independent of \( R \) (see Appendix I, Theorem 3). Fig. 7 shows the probability density function of \( SIR^{-1} \), random variable in a slot with up to four interferers for the free space propagation model.

The broadcaster’s success probability can be found by integration of the given pdfs over the interval \([0, 1/T_r]\). Having only one interferer and with a regular \( T_r \) equal to 10dB, the probability of successful decoding is only 0.05 and this value reduces to 0.0027 for 10 interferers. Later in Eq. (14), these small values will be multiplied by the probability of such occurrences too. Since high number of transmissions both leads to very small success probability and usually has small probability of occurrence, one can limit the maximum number of interfering transmissions in the analysis to a certain value like \( M (M \leq N - 1) \) by approximation. The tree of possible conditions of Eq. (16) is depicted in Fig. 8. The tree shall only account for those chains of events in which new interferers are added and previous ones vanish in forward moves. The pair \((i, j)\) in each leaf means that \( i \) new interferers are added with respect to the previous effective event and \( j \) interferers are still present out of \( n_0 \) initial interferers at time \( t \). There are multiple trees of this kind as \( n_0 \) can vary from 0 to \( M \). The maximum depth of these trees is \( \min(L, M + 1) \). Once the trees are constructed for the pair \((L, M)\), they can be reused for any design configuration with \( L' \leq L \), \( M' \leq M \) too.

The integrals, corresponding to the leaves, are invariant to the network parameters other than \( T_r \) and hence the tree can be constructed once for large \( L \) and \( M \) in an offline manner and be stored to be used by every designer.

Eq. (17) gives an expression for the overall number of leaves these trees have. We denote this quantity by \( N_T \). As the largest tree corresponds to \( n_0 = M \), the number of leaves is of \( O(M^{2L-1}) \) if \( M \geq L \).

\[ N_T = (M + 1) \]

\[ + \sum_{n_0=0}^{M} \sum_{n_1=0}^{M-n_0} M - n_1 \]

\[ + \sum_{n_0=0}^{M} \sum_{n_2=0}^{M-n_0} \sum_{n_3=0}^{M-n_1} M - (n_2 + n_3) + \cdots \]

\[ + \sum_{n_0=0}^{M} \sum_{n_2=0}^{M-n_0} \sum_{n_3=0}^{M-n_1} \sum_{n_4=0}^{M-n_2} \sum_{n_5=0}^{M-n_3} \sum_{n_6=0}^{M-n_4} \cdots \]

\[ L \geq 2 \]

\[ M-(n_2+n_4+\cdots+n_2(L-2)-2+n_2(L-2)-1) \]

\[ n_2(L-1)-3 \]

\[ - (n_2 + n_4 + n_6 + \cdots + n_2(L-2) + n_2(L-2)+1) \]
V. MODEL VALIDATION AND DISCUSSION

To validate the proposed theoretical model, we have developed code using C++. The CSMA/CA contention protocol implemented complies with the IEEE 802.15.4 MAC layer standard specifications (with CW=1). The broadcasting scenarios were simulated using Monte Carlo method as practical references for comparisons. For each payoff measurement, the experiment was repeated at least 2000 times and the mean values were computed. For simplicity in evaluations, we ignored the randomness of the number of the nodes in the affected area by always deploying the mean number \( N = \pi R^2 \delta \).

Since there are wide ranges of parameters involved \( \left( BE_{\text{min}}, BE_{\text{max}}, NB_{\text{max}}, N \right) \), \( L \), \( r_{cs} \), \( T_r \), demonstration of the whole model functionality is impossible. However, for a few reasonable sets of parameters we compare the theoretical and practical results. The default parameter values used in the evaluations are listed in Table I. For the medium, we chose the free-space propagation model. The benign transmission power \( P_{tx} \) along with the minimum reception power \( P_{rx} \) and the carrier sense power \( P_{cs} \), determine \( r_{rx} \) to be 20m and \( r_{cs} \) to be 96.8m in this model.

To validate the proposed theoretical model, we have been plotted alongside the theoretical curve obtained from the analysis of Section III. In the benign scenario (Fig. 9), the number of contenders is small. The channel busyness probability at the beginning of the contention is rather high but the curve shows a fast decrease afterwards. This is due to fact that the initial backoffs are rather short and the probability that the nodes transmit in the initial timeslots is very high. Fig. 10 demonstrates the channel busyness probability in an attacked scenario. In the initial timeslots, the number of contenders is very high. Starting from timeslot one, since the initial backoff exponents are rather small, many of the nodes choose similar backoff periods. Therefore, the channel is initially made almost busy by those who have chosen timeslot one to perform their first CCA. After the transmissions of this group of nodes are finished, the channel remains free for one timeslot since any other node in the previously busy area needs to do CCA before commencing transmission. This phenomenon creates valleys in the channel busyness curve repeatedly until the number of contenders is significantly decreased.

In another evaluation, the transmission range of the broadcaster was swept from the benign range to longer ones representing attack scenarios and the practical payoff values were compared with the results obtained from Section IV analysis. Fig. 11 shows that longer packets will result in lower maximum payoffs. This is due to the fact that longer packets will create more interference for the other packets. However, the mean number of decodable reply packets does not show any noticeable change at the benign range since at this range there is enough statistical separation between the packets with the given timings.

Positive errors in the short broadcast ranges are a result of model simplifications. According to the CCA mechanism, there must be a gap between every two possible successive packets whose transmitters are in the carrier sense range of each other. Due to the stochastic nature of the model in temporal analyses, sometimes the probability of such incident is non-zero which implicitly means giving more chance to the broadcaster to virtually receive packets with lower interference. As it can be seen in Fig. 11, this error is not relatively high especially when \( L \) is not too small.

At the other side, the negative errors in high broadcast ranges mainly originate from two sources: the limitation in the depth of payoff analysis \( (M) \) which introduces an always-

Table I- Nominal parameters values used for simulations

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>2.4GHz</td>
</tr>
<tr>
<td>( P_{tx} )</td>
<td>3.652e-10w</td>
</tr>
<tr>
<td>( P_{cs} )</td>
<td>1.559e-11w</td>
</tr>
<tr>
<td>( P_{tx} )</td>
<td>0.0015w</td>
</tr>
<tr>
<td>( BE_{\text{min}} )</td>
<td>5</td>
</tr>
<tr>
<td>( BE_{\text{max}} )</td>
<td>6</td>
</tr>
<tr>
<td>( NB_{\text{max}} )</td>
<td>3</td>
</tr>
<tr>
<td>( \delta )</td>
<td>0.004 m²</td>
</tr>
<tr>
<td>( L )</td>
<td>5</td>
</tr>
<tr>
<td>( T_r )</td>
<td>10dB</td>
</tr>
</tbody>
</table>

Fig. 9 and Fig. 10 show the channel busyness probability for \( R = 20m \) (the benign scenario) and \( R = 300m \) (an attack scenario) respectively. In each case, the simulation result has been plotted alongside the theoretical curve obtained from the analysis of Section III. In the benign scenario (Fig. 9), the number of contenders is small. The channel busyness probability at the beginning of the contention is rather high but the curve shows a fast decrease afterwards. This is due to fact that the initial backoffs are rather short and the probability that the nodes transmit in the initial timeslots is very high. Fig. 10 demonstrates the channel busyness probability in an attacked scenario. In the initial timeslots, the number of contenders is very high. Starting from timeslot one, since the initial backoff exponents are rather small, many of the nodes choose similar backoff periods. Therefore, the channel is initially made almost busy by those who have chosen timeslot one to perform their first CCA. After the transmissions of this group of nodes are finished, the channel remains free for one timeslot since any other node in the previously busy area needs to do CCA before commencing transmission. This phenomenon creates valleys in the channel busyness curve repeatedly until the number of contenders is significantly decreased.

In another evaluation, the transmission range of the broadcaster was swept from the benign range to longer ones representing attack scenarios and the practical payoff values were compared with the results obtained from Section IV analysis. Fig. 11 shows that longer packets will result in lower maximum payoffs. This is due to the fact that longer packets will create more interference for the other packets. However, the mean number of decodable reply packets does not show any noticeable change at the benign range since at this range there is enough statistical separation between the packets with the given timings.

Positive errors in the short broadcast ranges are a result of model simplifications. According to the CCA mechanism, there must be a gap between every two possible successive packets whose transmitters are in the carrier sense range of each other. Due to the stochastic nature of the model in temporal analyses, sometimes the probability of such incident is non-zero which implicitly means giving more chance to the broadcaster to virtually receive packets with lower interference. As it can be seen in Fig. 11, this error is not relatively high especially when \( L \) is not too small.

At the other side, the negative errors in high broadcast ranges mainly originate from two sources: the limitation in the depth of payoff analysis \( (M) \) which introduces an always-
negative error, and the transmitters’ distances independence assumption. The former error can be reduced at the cost of computational complexity increase. As we mentioned before, even a single interference reduces the chance of correct reception to about 5%. Since this error is determinist only when the timings are so tight (with respect to $N$) that there are many overlapping transmissions, its strong presence in the most interesting point of the curve which is the peak is ruled out.

Fig. 12 and Fig. 13 show how the payoff curves change with $BE_{\text{min}}$ and $BE_{\text{max}}$. Increasing the values of these two parameters at a given range and with a given packet length, causes spreading of the same number of packets over a longer interval thus lowering the chance of collisions which in turn increases the payoff. Uncontrolled increase of these parameters will dramatically increase both the delay and the adversary’s maximum achievable payoff. Changes of $BE_{\text{min}}$ does not significantly move the range at which the maximum payoff is obtained however the maximum payoff value is significantly affected. Smaller $BE_{\text{min}}$ means starting from shorter jumps, which increases the collisions in the initial time-slots. Longer exponential jumps in the last backoffs create the opportunity for more nodes to transmit their packets with low probability of collision. So increasing $BE_{\text{max}}$ gives rise to the maximum achievable payoff and also moves it toward higher ranges (corresponding to larger $N$).

Irrespective of how the designer sets the network and protocol parameters, the theoretical model predicts the payoff curve behavior well, especially the range at which the adversary gains most.

VI. APPLICATIONS

The model developed in this paper is useful for both network design engineers and attackers. As shown in the previous section, with a given packet length, to have less collisions at the benign range, the timing parameters are set in such a way that allow the packets to be distributed over a reasonable number of slots using random binary exponential backoffs. Due to the nature of random channel accessing protocols, the number of timeslots needed for reply data transmissions with low collision probability, is more than the number of nodes involved multiplied by the length of the packets. So it is expected that with the initial increase in the broadcast range (which increases $N$), the free slots are filled up with more packets and the adversary’s payoff is increased. However, as the timing parameters are fixed, further increase of $R$, adds more responders to the system whose packets start to overlap and collide at the receiver and consequently the payoff curve shows a downward trend afterward.

The concavity of the payoff curve is interesting for the flooding attackers, as for a given set of parameters, only at a certain range they benefit most (see Fig. 11, Fig. 12 and Fig. 13). The set of parameters affecting the adversaries’ payoff can be summarized as $\{BE_{\text{min}}, BE_{\text{max}}, NB_{\text{max}}, \delta, L, P_{\text{tx}}, P_{\text{cs}}, T_{\text{r}}, R\}$. $T_{\text{r}}$ and $R$ are designer-uncontrolled variables and will be determined by the attacker. The model can be used to give an estimation of the optimal attack range for the adversaries prior to deployment.

On the other hand, a network architecture designer who wants to evaluate the probability of success in benign broadcast challenges, can use the proposed model to estimate how well a given set of parameters will do in reality. From the designer’s point of view, the main concerns are efficiency (low collision), energy consumption, security, and in some applications the data collection delay. To have a low
probability of collision, the timing parameters should provide a proper long transmission interval while low-delay applications and flooding-related security concerns enforce tighter timings.

The proposed model can help a designer to protect the network against flooding adversaries using statistical techniques at a low cost. Preventive solutions are the most effective means of providing security. According to game theory, the rules themselves prevent rational players from taking actions which reduce their payoffs [35]. Therefore, the network parameters can be optimized so that maintaining an acceptable level of efficiency at the benign range, the maximum achievable payoff of any potential flooding adversary is kept minimal. To counteract the adversary’s greediness, the designer has to embed some valuable information into the nodes’ responses so that without these, future communications with the nodes become impossible. Examples of these valuable data are mutual key constructing information into the nodes’ responses so that without these, maximum achievable payoff of any potential flooding is not possible when black color. For the given settings and within the range shown which result in an efficiency of \( \alpha \geq 0.9 \). We define \( \alpha = n_a/n_b \) to be the measure of efficiency at the benign range. Let us denote the mean number of neighbors the adversary obtains by \( n_a \) \( (n_a \geq n_b) \). The quantity \( \beta = (n_a - n_b)/n_b \) is defined to be the penalty paid by the designer which is the gap between the optimal mean number of neighbors in benign scenarios and the adversary’s maximum payoff. The MAC protocol parameters can be tuned in such a way that providing a reasonable value of \( \alpha, \beta \) is kept minimal. In [19], without optimization of the parameters and for a specific setting, we had shown by means of simulation that in a neighbor discovery scenario based on a modified IEEE 802.15.4 MAC protocol, the penalty can be kept as low as \( \beta = 0.5 \) maintaining an efficiency of \( \alpha = 0.88 \). Fig. 14 shows the model-derived values of the penalty sweeping the values of \( L \) and \( n_b \) for the settings given in Table I. The pairs which result in an efficiency of \( \alpha \geq 0.9 \) are distinguished by black color. For the given settings and within the range shown for \( L \), one can easily deduce that providing an acceptable level of benign operation efficiency is not possible when \( n_b \) (or equivalently the deployment density) goes above a threshold. Moreover, the penalty decreases with both the increase of density and the increase of packet length.

In another scenario, assuming that \( L \) is determined by the design constraints, we used the model as a tool in finding the optimal timing settings and the deployment density, which minimize \( \beta \) satisfying \( \alpha \geq 0.9 \). This can be an example of the problem a designer with security concerns faces. We used the timing ranges recommended in the IEEE 802.15.4 standard [31], i.e. \( 0 \leq BE_{\text{max}} \leq 8 \), \( 0 \leq BE_{\text{min}} \leq BE_{\text{max}} \), \( 0 \leq NB_{\text{max}} \leq 5 \). We searched for \( n_b \) among natural numbers greater than three (\( n_b \geq 3 \)) to avoid network graph being disconnected. Other parameters were set according to Table I. The model was fast enough to allow an exhaustive search. For broader domains, evolutionary algorithms also showed very promising results in our experiments. Table II shows the optimal settings for four values of the packet length (\( L \)). It is interesting to note that the optimal density is the same for all the packet lengths shown in the table. The \( \{BE_{\text{min}}, BE_{\text{max}}\} \) pair optimal values reveal that fixed backoff window sizes perform better than binary exponential ones in creating statistically flood-resilient MAC protocols. The penalty decreases with the increase of packet length as expected. The table shows that the penalty can be kept as low as \( \beta = 0.74 \) when \( L = 9 \) while the benign operation efficiency is still \( \alpha \geq 0.9 \).

In highly mobile networks, the neighbor discovery timeliness (or data collection delay) is critical. In such cases, no cryptographic solution is able to counteract internal flooding as cryptographic solutions rely on key establishments between local neighbors once at the beginning of the operation of the network whose structure is not fixed and is ever-changing in this case [21]. Distance bounding solutions will also be of limited use since aside from the imposed delay, they usually rely on the location information and time-stamps provided by the interacting nodes in order to protect the network against external attackers [21]. Even energy-consuming topology verification methods like graph abnormality tests are subjected to high false positive and false negative alarms due to the rapidly changing graph. The statistical countermeasure is valuable since it is well applicable in mobile networks and besides, does not rule out employment of other security solutions and can be used in combination with them.

VII. CONCLUSION

Many of the current information acquisition and routing algorithms rely on broadcasting challenge-response sub-protocols. Modeling the channel and finding the broadcaster’s payoff in each run of such protocols are of great importance.

![Fig. 14. The model-derived values of the penalty (β) sweeping L and n_b for BE_{min} = 5, BE_{max} = 6, NB_{max} = 3, \text{ and } r_{tx} = 20\text{m and } r_{cs} = 96.8\text{m.}](image-url)
The traffic burst that occurs after the issuance of the challenge requires non-stationary modeling of the channel. The previous studies did not model the malicious flooding scenarios. In this paper, we have proposed a recursive time-domain model for finding the effective channel busyness probability along with a method to estimate the broadcaster’s payoff, supporting both benign and malicious scenarios. In discussing the applications of the proposed model, we have described how it can be used to work out the estimation of the optimal attack range for the attackers and development of a flood-resilient MAC protocol that increases the security of neighbor discovery protocols using statistical techniques; this is especially relevant in the case of mobile networks where cryptographic solutions are costly or even infeasible to employ. We have also addressed the optimization problems with the MAC protocol and specified the network parameters the network designer deals with in the objective function. Guaranteeing a certain given level of efficiency for the benign broadcast range, the goal in the Hello flooding case is to minimize the maximum achievable payoff in malicious scenarios while in highly mobile networks the objective function is mainly influenced by the data acquisition delay index.

REFERENCES


Appendix I

Theorem 1. Having \( m - 1 \) transmitters inside a circle of radius \( R \) with \( \forall i, j \in \{1, \ldots, m-1\}, i \neq j: d_{ij} > r_{cs} \), the probability that the \( m^{th} \) node chosen inside the circle satisfies \( \exists k \in \{1, \ldots, m-1\} : d_{km} \leq r_{cs} \) is invariant to the changes of \( R \) and \( r_{cs} \) as long as \( \eta \) is fixed.

Proof:
Let \( (x_i, y_i) : i = 1, \ldots, m \) be the set of \( m \) points coordinates (which satisfy \( \forall i: x_i^2 + y_i^2 \leq R^2 \)) and \( Y_{x, y}^{r_{cs}} \) be the event that the \( m^{th} \) point distance to at least one of the points is smaller than \( r_{cs} \). We can write:

\[
P(Y_{x, y}^{r_{cs}}) = 1 - P(Y_{x, y}^{r_{cs}}^c)
\]

\[
Y_{x, y}^{r_{cs}} = \{ (x_i, y_i) : i \neq j \}
\]

\[
P(Y_{x, y}^{r_{cs}}^c) = \frac{\pi R^2}{\sqrt{2\alpha}} \prod_{i=1}^{m-1} \int_0^{\pi} \int_0^{\pi} \alpha d\alpha d\eta
\]

Theorem 2. Let \( (x_i, y_i) : i = 1, \ldots, m-1 \) be the Cartesian coordinates of \( m - 1 \) nodes uniformly distributed inside a circle of radius \( R \). The probability that the \( m^{th} \) node chosen randomly inside the circle satisfies \( \exists k \in \{1, \ldots, m-1\} : d_{km} \leq r_{cs} \) is invariant to the changes of \( R \) and \( r_{cs} \) as long as \( \eta \) is fixed.

Proof:
Let \( (r_i, \theta_i) : i = 1, \ldots, m \) be the polar coordinates of uniformly distributed points \( (x_i = r_i \cos \theta_i, y_i = r_i \sin \theta_i) \). Then the joint pdf of \( r_i \) and \( \theta_i \) is:

\[
f_{r_i, \theta_i}(r_i, \theta_i) = \left\{ \begin{array}{cl}
\frac{r_i}{\pi R^2} & 0 \leq r_i \leq R; \ \theta_i \in [0, 2\pi] \\
0 & \text{others}
\end{array} \right.
\]

(22)

Let \( Y_{r, \theta}^{r_{cs}} \) be the event that the \( m^{th} \) point distance to at least one of the points is smaller than \( r_{cs} \). We can write:

\[
P(Y_{r, \theta}^{r_{cs}}) = 1 - P(Y_{r, \theta}^{r_{cs}}^c) = 1 - \int_0^{\pi} \int_0^{\pi} g \left( \frac{u^2 + v^2 - a^2}{2uv} \right) 2udu dv
\]

(23)

(24)

where we have changed the variables \( \nu = \rho_i / R, r = r_{cs} / R \) and \( u = \rho_i / R \) and according to Eq. (22), \( f_\theta(u) = 2u; 0 \leq u \leq 1. \) Since \( \theta_i - \theta_m \) is also uniformly distributed over \([0,2\pi]\), we may write:

\[
P(\cos(\theta_i - \theta_m) < \frac{u^2 + v^2 - a^2}{2uv}) = P(\cos(\theta_i - \theta_m) < \frac{u^2 + v^2 - a^2}{2uv})
\]

(25)

Thus the probability we were after is:

\[
P(Y_{r, \theta}^{r_{cs}}) = 1 - \int_0^{\pi} \int_0^{2\pi} g \left( \frac{u^2 + v^2 - a^2}{2uv} \right) 2udu dv
\]

(26)

which is clearly independent of \( R \) and the proof is completed.

Theorem 3. Assuming transmitters’ distances to the receiver to be continuous independent random variables with \( f_r(r) = 2rR^2; 0 \leq r \leq R \), the signal to interference ratio is invariant to the broadcast range \( R \).

Proof:
Let the propagation model be defined by the following generic equation:

\[
P_{tx} = K \frac{1}{d^n}
\]

(27)
where $d$ is the distance between the transmitter and receiver, $n$ is the path loss exponent, $K$ is a constant and $P_{tx}$ and $P_{rx}$ represent the transmission and reception powers respectively. Using Eq. (27) we can rewrite the generic signal to interference term $\varphi_{e_i}^j$ as:

$$\varphi_{e_i}^j = \frac{1}{r_i^n} \frac{1}{\sum_{k \in I} r_k^n}$$  \hspace{1cm} (28)

where $I$ is the set of interfering nodes’ indexes having tails on the $j$th effective slot of the $i$th node. With the independence assumption, the distribution of distances is given in Eq. (11) and we have:

$$y_0 \overset{d}{=} \frac{r_i}{r_k}, \quad y_1 \overset{d}{=} r_k$$

$$f_{y_0y_1}(y_0, y_1) = f_{r_ir_k}(y_0y_1) / l = \frac{4y_0y_1^3}{R^4};$$

$$0 \leq y_0 y_1 \leq R, \quad 0 \leq y_1 \leq R$$

$$f_{y_0}(y_0) = \int_{\min(R/y_0, R)} f_{y_0y_1}(y_0, y_1) dy_1$$

$$= \int_{0}^{\min(R/y_0, R)} \frac{4y_0y_1^3}{R^4} dy_1$$

$$f_{y_0}(y_0) = \begin{cases} y_0 & 0 \leq y_0 \leq 1 \\ \frac{1}{y_0} & y_0 > 1 \end{cases}$$  \hspace{1cm} (29)

And hence, $\frac{r_i^n}{r_k^n}$ and in the next level $\varphi_{e_i}^j$ are also invariant to $R$.

Mohammad Sayad Haghighi received his B.Sc. in electrical engineering at Telecommunication College (PTT) in 1979. After receiving the M.Sc. degree in electrical engineering from University of Tarbiat Modaress in 1987, he pursued his study in Ph.D. level in the same field in UK. He received his Ph.D. from the University of Manchester in 1996. His research interests include cellular/mobile communication, MIMO, OFDM and digital signal processing.

Vijay Varadharajan currently holds the Endowed Microsoft Chair Professor in Innovation in Computing. He is also Director of Information and Networked System Security Research at Macquarie University, Australia. Prior to joining Macquarie University, he was Foundation Professor and Chairman of School of Computing and IT at the University of Western Sydney; before this, Vijay was responsible for worldwide Security Research at corporate Hewlett-Packard Labs for over nine years based in European Headquarters of HP Labs. Before HP, he was Research Manager at British Telecom Research Labs U.K. Professor Varadharajan has published more than 320 papers in international journals and conferences, has co-authored and edited eight books on security, networks and distributed systems and holds four patents. His current areas of research interest include security for large distributed systems and cloud infrastructures, security in mobile and high speed networks, Internet security, trusted computing and systems, secure mobile computing, security and privacy in peer to peer distributed applications and security models and architectures.

Barry G. Quinn received the B.A. Hons. degree in pure mathematics, applied mathematics, and statistics in 1978 and the Ph.D. degree in statistics in 1981, both from the Australian National University, Canberra. He is currently Professor of Statistics and Head of the Statistics Department with Macquarie University, Sydney. He has previously held Professorships at UMIST (now part of the University of Manchester, U.K.) and Goldsmiths College, London, U.K. He has also held lectureships with the Universities of Wollongong, Queensland, and Newcastle, and was a Principal Research Scientist with DSTO, Adelaide. His interests are in time series analysis and signal processing, and especially frequency estimation.

Kamal Mohamedpour is an associate professor in telecommunications with the department of electrical engineering at K. N. Toosi University of Technology. He finished his B.Sc. in