Computer Networks 53 (2009) 382–399

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

The impact of a realistic packet traffic model on the performance of surveillance wireless sensor networks

Ilker Demirkol [a], Cem Ersoy [a,*], Fatih Alagöz [a], Hakan Deliç [b]

[a] Computer Networks Research Laboratory, Department of Computer Engineering, Boğaziçi University, Bebek 34342 Istanbul, Turkey
[b] Wireless Communications Laboratory, Department of Electrical and Electronics Engineering, Boğaziçi University, Bebek 34342 Istanbul, Turkey

ARTICLE INFO

Article history:
Received 4 May 2008
Received in revised form 18 October 2008
Accepted 26 October 2008
Available online 7 November 2008

Responsible Editor: H.S. Hassanein

Keywords:
Packet traffic model
Wireless sensor networks
Surveillance sensor networks
Intrusion detection applications

ABSTRACT

It is quite common to see that classical periodic or Poisson packet traffic models are used for evaluating the performance of wireless sensor networks (WSNs). However, these models may not be appropriate for modeling the data traffic resulting from a particular application. Furthermore, they may be overestimating the performance of a WSN. In this paper, we show the significance of using a realistic and application-specific packet traffic model by comparing the performance of a well-known WSN protocol under the Surveillance WSN packet traffic model (SPTM), as well as under periodic and binomial traffic models. A packet traffic framework specific to surveillance applications is proposed which is then used for deriving SPTM analytically. In order to be adaptable and flexible, SPTM incorporates a probabilistic and parametric sensor detection model. Simulation results show that to employ an application-specific packet traffic model has significant impact on the performance evaluation of the WSN and ordinary traffic models may overestimate the capacity of the WSN.

1. Introduction

Potential application areas of wireless sensor networks (WSNs) show contrasting properties which prevent the development of universal algorithms serving all purposes. Military applications may require very fast response time, whereas in agriculture, delay sensitivity may be traded with energy conservation. Likewise, a communication protocol may perform in a very energy-efficient manner when used for one application, and it may perform quite poorly in another. One application-dependent characteristic of a WSN is the type of data traffic generated by the nodes. The model that represents the aggregate packet traffic in the network or a cluster of the network can be used to determine the maximum stable throughput, expected delay and the packet loss characteristics. Furthermore, the effects of parameters such as node density and target velocity can be investigated in depth once an appropriate data traffic model is available.

When communication protocols are developed without taking into account the properties of the data traffic, they may behave inefficiently. In the WSN literature, the performance evaluation of the protocols are generally carried out with periodic data traffic as in [1–3], or using common data traffic models such as Poisson point processes [4–6]. However, event-driven applications such as target detection and tracking produce bursty traffic which cannot be modeled as either periodic or Poisson [7]. Although there are packet traffic models available for legacy communication networks, the unique features and requirements of WSNs call for the design and development of dedicated models. For instance, the limited battery capacity necessitates the use of sleep-listen periods and sensing intervals to extend the lifetime of the network.

In this paper, we investigate the importance of using a realistic packet traffic model by deriving a specific surveillance WSN packet traffic model (SPTM) and comparing the performance of a WSN medium access control (MAC)

* Corresponding author. Tel.: +90 2123596861; fax: +90 2122872461.
E-mail addresses: ilker@boun.edu.tr (I. Demirkol), ersoy@boun.edu.tr (C. Ersoy), alagoz@boun.edu.tr (F. Alagöz), delic@boun.edu.tr (H. Deliç).

1389-1286/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.comnet.2008.10.021

List of symbols

Symbol	*Definition*
$\varphi(d)$	probability of detection of a target at distance d
α	Elfes detection parameter
β	Elfes detection parameter
θ	angular coordinate of the sensor when the pole is set to the target location
γ	probability of detection for any one sensor within the d_u-distance of the target
$\rho_{\max}$	maximum stable throughput
ζ	probability of packet collision in a contention period
Ψ	random variable of the index of the first occupied slot
ξ	probability that a slot assignment results in a collisionless transmission
a	Gauss–Markov mobility model randomness parameter
$\mathscr{C}_i$	location of target at instance i
c_i	coverage degree at point $\mathscr{C}_i$
$c_{x,y}$	coverage degree at point x,y, i.e. the number of sensor nodes that have positive detection probability for a target at x,y
$\mathscr{D}_i$	disk whose center is at $\mathscr{C}_i$ and whose radius is d_u, i.e. the coverage area of a the sensor at location $\mathscr{C}_i$
d_u	sensing range
d_c	certain detection range
$\mathscr{E}$	direction of the mobile in Gauss–Markov mobility model
$\mathscr{F}$	random variable that represents the index of first occupied slot given that it is selected by only one node
$\mathscr{K}_i$	random variable that represents the detection degree of the event point $\mathscr{C}_i$
k_i	detection degree at point $\mathscr{C}_i$
$k_{x,y}$	detection degree at point x,y, i.e. the number of sensor nodes that detects the target at x,y
L	border length
$\mathscr{M}$	number of contending nodes
N	number of sensors
p	probability that a deployed node is within the d_u-distance of the target point
r	radial coordinate of the sensor when the pole is set to the target location
$\mathscr{S}$	speed of the mobile in Gauss–Markov mobility model
t_{coll}	time spent for the collided packets' transmissions
t_{CW}	time spent for waiting the first occupied contention slot
t_{listen}	listen period in seconds
t_X	time needed for the transmission of a packet type X where X is RTS, CTS, DATA or ACK.
t_s	sensing interval
t_{slot}	one slot duration
t_{stx}	time required for a successful packet transmission
v_T	target velocity
W	border width
$\mathscr{X}_i$	number of sensor nodes that have non-zero detection probability, i.e. the sensor nodes that resides within the d_u-distance of the event point $\mathscr{C}_i$
$\mathscr{Y}_i$	number of nodes that reside in $\mathscr{A}_i$
$\mathscr{Z}$	number of contention slots in a contention window
z	number of successive collisions

protocol under different packet traffic models. We show that the underlying packet traffic model can result in dissimilar performance results for the same average packet traffic loads. This observation is significant because the improper packet traffic models may result in underestimated or overestimated performance results and lead to inefficient protocol design and implementation.

In the WSN literature, the application-specific packet traffic models are not studied extensively. In [8], the traffic generated by a single WSN node connected to a body temperature or an electrocardiogram sensor is investigated for medical applications. The traffic traces of an intrusion detection scenario are studied in [9], where numerical function fitting is carried out for the total number of packets generated at any instance. However, no generalized analytical model is derived. An analytical packet traffic model for intrusion detecting WSN is investigated in [7] in which binary sensor detection is assumed. However, binary detection is an idealized model in which the detection probability is defined with only a single parameter. To achieve a more configurable and potentially more realistic packet traffic, a probabilistic detection model is employed in this work which includes a set of parameters to define the range-based detection probabilities. These detection parameters can be set according to the physical properties of the sensors deployed and of the potential targets. Based on this probabilistic detection model, we introduce a framework for the SPTM and derive the analytical formula for its components. The derived SPTM model is used to corroborate how a realistic packet traffic modeling makes a difference.

In Section 2, we describe the packet traffic framework that is used for the SPTM and present an analytical model for the proposed framework. Then, in Section 3, we verify the introduced analytical model with simulations. In Section 4, packet traffic generation algorithms are presented based on the proposed analytical packet traffic model. The performance evaluation results of the well-known S-MAC protocol [10] are compared for SPTM, as well as the periodic and the binomial packet traffic models in Section 5. Finally, Section 6 includes the analytical derivations of the maximum stable throughput to verify the simulation results. A list of symbols used in the mathematical equations are given at the end of the text.

2. Surveillance wireless sensor networks packet traffic model

Surveillance wireless sensor networks (SWSN) represent the WSN applications in which the deployed sensor nodes monitor an area such as border for potential intruder entrance. When an intrusion is detected, the detecting sensors send data packets to the sink so that the necessary actions can be taken. Such a network can be employed for security applications, habitat monitoring, or disaster management applications. Because of the distinctive properties of these applications, the generated data are bursty and require a specific packet traffic model.

2.1. SWSN packet traffic model (SPTM) framework

Packet traffic models can be represented by a Markov process where the *state* $\tilde{s}$ corresponds to the event that s data packets are generated by the sensing nodes at a given data generation instant which are mainly the sensor sampling instances for surveillance networks. The state transition probability from *state* $\tilde{a}$ to *state* $\tilde{b}$ indicates the probability of generating b data packets with the knowledge of a data packets generated at the previous sampling instant. The dependency between the number of packets generated at the successive sampling instances determines the order of the Markov process. The order is zero for memoryless packet traffic models such as Poisson and periodic data traffic, i.e. the probability of a transition to *state* $\tilde{b}$ is independent from the current state. For SPTM, the order is a positive value depending on the properties of the intruder movements and sensor node attributes which is formulated in [7]. The dependency in subsequent number of detections is represented in Fig. 1. The cross shaded sensors in Fig. 1 detect the target in the two consecutive sampling instances, and hence, generate data packets in both sampling instances. The subsequent set of detecting sensors is determined by the target velocity and the sensing interval of the sensors, t_s.

Since radio communication and sensing are two separate power consuming operations for sensors,[1] each has its own duty cycle. The duty cycles can be static or can be increased dynamically in case of event presence. For either case, assume that the sensing duty cycle interval is t_s in the presence of a target, which means that each node senses the environment once in t_s seconds. Hence, after the target is detected by a sensor at location (x, y) at time t, it will possibly be detected by the same node again at location (x', y') at time $t + t_s$, where the Euclidian distance between (x, y) and (x', y') is $v_T t_s$, with v_T being the velocity of the target within the $(t, t + t_s)$ period as illustrated in Fig. 1. When one data packet is created at each target detection, assuming that the sensing offset of all sensors are the same, the number of data packets generated at point (x, y) is equal to the *detection degree* of that location, $k_{x,y}$, which is defined as the number of sensor nodes that actually detect the event.[2] Hence, a realistic packet traffic model for an SWSN application should provide the probability mass function (PMF) of the detection degree given the previous detection degree.

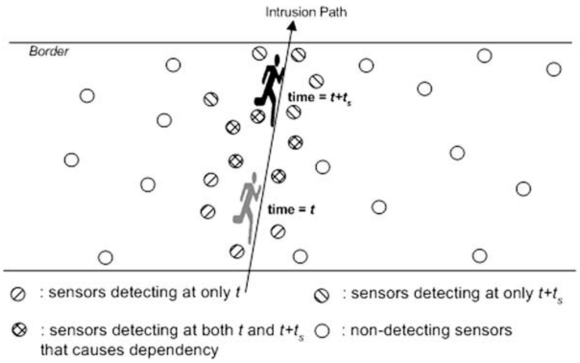

Intrusion Path
Border
time = t+t$_s$
time = t
⊘ : sensors detecting at only t
⊘ : sensors detecting at only t+t$_s$
⊗ : sensors detecting at both t and t+t$_s$ that causes dependency
○ : non-detecting sensors

Fig. 1. Illustration of the dependency between subsequent number of detections where t_s is the sensor sampling period.

The assumption of sensing offset synchronization is acceptable since for successful communication of the sleeping neighboring nodes, time synchronization between them is always necessary. Time division multiple access (TDMA) based protocols require strict synchronization, however carrier sense multiple access (CSMA) based protocols, such as S-MAC, require looser synchronization. Hence, the sensing duty cycle can be synchronized using the communication cycle. Moreover, even if the communication and the sensing duty cycles are different, the corresponding detection packets will be transmitted at the beginning of the next communication duty cycle.

Different sensor detection models are proposed for sensor nodes [12]. The detection probability of an event by a sensor node is in general a function of the sensor-to-event distance. According to *the binary detection model*, an event occurring within a specific range (sensor range) of a sensor node is detected by that node with probability 1, and it is not detected, otherwise. In other words, for the binary detection model, the probability of the target detection by a sensor is

$$\varphi(d)\begin{cases} 1 & \text{if} \quad d \leqslant d_c, \\ 0 & \text{if} \quad d_c < d, \end{cases} \tag{1}$$

where d is the distance between the target and the sensor node and d_c is the threshold distance for detection, which is also called the sensing range.

Zou et al. [13] proposed a more general, probabilistic sensor detection model based on the Elfes' work [14]. Here, the dependency is parametric enabling the representation of different sensor types. Specifically, in the *Elfes sensor detection model*, the probability that a sensor detects an event at distance d is

[1] As a numerical example, Crossbow motes require 5 mA for the sensor board operations whereas 8 mA and 12 mA are required by the radio board for reception and transmission, respectively. However, when both boards are in sleep mode, they require only a few μA's [11].

[2] Since *intrusion detection* is investigated as the event-driven application, the terms *target detection* and *event* are used interchangeably.

$$\varphi(d) = \begin{cases} 1 & \text{if} \quad d \leqslant d_c, \\ e^{-\alpha(d-d_c)^{\beta}} & \text{if} \quad d_c < d < d_u, \\ 0 & \text{if} \quad d_u \leqslant d, \end{cases} \tag{2}$$

where d_c, d_u define the certainty and uncertainty boundaries in detection, respectively. To clarify the term *sensing range*, d_c can be called the certain detection range and d_u can be called sensing range, for the Elfes case. Hence, the target is detected with probability 1, if the target is within the certain detection range and it is detected with an exponential probability, if it is outside of the certain detection range but still within the sensing range. No detection occurs by the sensors that are further than the sensing range. The parameters α and β, as well as d_u, d_c, reflect the physical properties of the sensors. In particular, α and β determine the rate and region of decay in $\varphi(d)$. An alternative detection model that incorporates false alarm rate and additive white Gaussian noise is Neyman–Pearson detector [15]. However, the Elfes model can accommodate the Neyman–Pearson detector through proper parameter matching as indicated in [16].

Calculation of the total number of detecting sensor nodes, $d_{x,y}$, requires the knowledge of the number of sensor nodes that have positive detection probability, which is called the coverage degree and represented as $c_{x,y}$ for the detection point (x, y). For an event location, a subset of the nodes with positive detection probability will detect the event. Therefore, the coverage degree of a location is always greater than or equal to its detection degree. For the Elfes model, the sensor nodes that have positive detection probability are those within d_u distance of the event point, and for the binary detection model, they are the nodes within d_c distance. In addition, with the Elfes model, the locations of the sensor nodes determine the probabilities of the number of detections, since the detection probability is a function of the target distance for each sensor. Hence,

(1) The number of detecting sensor nodes (detection degree) is always less than or equal to the number of sensor nodes that have a positive detection probability (coverage degree), i.e. $k_{x,y} \leqslant c_{x,y}$.
(2) For the binary detection model, the detection degree is always equal to the coverage degree, i.e. $k_{x,y} = c_{x,y}$.
(3) The Elfes model reduces to the binary detection model, if $d_u = d_c$, and as a result, it enables more general and flexible sensor detection modeling.

The framework for SPTM is shown schematically in Fig. 2 and described as follows. As the target crosses the border, it can be detected by the sensor nodes deployed to the border which sample the environment periodically, i.e. once in t_s seconds. Hence, to find the number of data packets generated because of the target detections at the location (x, y), we first need to know the number of nodes that can detect the target at (x, y) which is the coverage degree of that location, $c_{x,y}$. Once we have the coverage degree, we then need to calculate the detection degree, $k_{x,y}$, based on $c_{x,y}$. Hence, for consecutive number of detections, we have to know the dependency between the coverage degrees of the target locations at consecutive sampling times. The main components of the framework are (i) the coverage degree, (ii) the detection degree, (iii) relation between the detection degree and the coverage degree (arrow 1), and (iv) the dependency of successive coverage degrees (arrow 2). The analytical derivations of these components are given in Section 2.2.

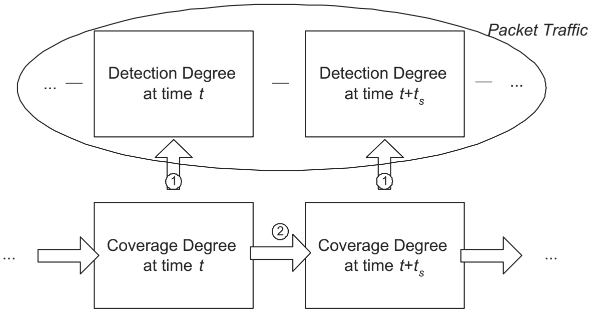

Packet Traffic
...
Detection Degree at time t
Detection Degree at time t+t_s
...
1
1
...
Coverage Degree at time t
2
Coverage Degree at time t+t_s
...

Fig. 2. SWSN packet traffic model (SPTM) framework.

2.2. Analytical model of the SPTM framework

In the WSN literature, two types of deployment are assumed in general: random deployment (e.g. [17,18]) and grid deployment (e.g. [19,20]). In *grid deployment*, nodes are placed deterministically along grid points, while in *random deployment* they are placed randomly in the application area. In this paper, we assume uniformly random deployment. However, we use the probabilities of the number of sensor nodes deployed within a specific area instead of setting the individual locations randomly. That enables the calculation of the coverage degree of the event locations without generating the whole deployment map.

Since $c_{x,y}$ is defined as the number of sensor nodes that has a positive probability to detect the target at (x, y), the PMF of $c_{x,y}$ is determined by the probability of the total number of sensors within the distance d_u of (x, y). However, as the surveillance area and the total number of sensors deployed within its borders are known, for each sensor node deployment, the event that the deployed node is within the d_u-distance of the target point is a Bernoulli trial with the probability of success $p = \pi d_u^2/LW$, where (L, W) is the length and width of the borders of the surveillance area. Hence, the total number of sensor nodes within distance d_u of a point forms a Binomial distribution. Moreover, for large number of retrials and small success probability, Binomial distribution can be approximated by a Poisson distribution. This is generally the case for intrusion detection applications, since the number of deployed sensors, N, gives the number of retrials and the probability that a deployed node resides within the d_u-distance of the target point, p, is small because of the large deployment area. The mean of the equivalent Poisson distribution is

$$\lambda = Np = \frac{N\pi d_u^2}{LW}. \tag{3}$$

The coverage degree probabilities of area points, hence, form a Poisson PMF. However, as illustrated in Fig. 1, because the number of sensor nodes within the sensing

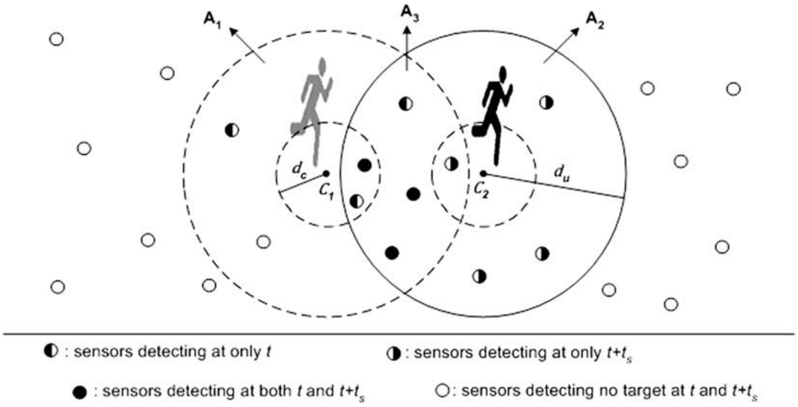

A1
A3
A2
d_c
C_1
C_2
d_u
◐ : sensors detecting at only t
◑ : sensors detecting at only $t+t_s$
● : sensors detecting at both t and $t+t_s$
○: sensors detecting no target at t and $t+t_s$

Fig. 3. Geometric representation of successive target detection locations.

ranges are similar, the coverage degree probabilities of two nearby surveillance area points are not independent of each other. If we are given the coverage degree of the target location at time t, we cannot use the Poisson distribution with the mean value given in (3) to estimate the coverage degree of the target location at time $t + t_s$, which will be the next detection point.[3]

Fig. 3 shows the reason for the degree-dependency between the successive points. Let $\mathscr{C}_1$ and $\mathscr{C}_2$ denote locations of the target at times t and $t + t_s$, respectively. If the target velocity at time t is v_T, then the distance between $\mathscr{C}_1$ and $\mathscr{C}_2$ is equal to $v_T t_s$. In addition, the coverage degree of point $\mathscr{C}_1$ ($\mathscr{C}_2$) equals to the number of sensor nodes residing on $\mathscr{D}_1(\mathscr{D}_2)$, where $\mathscr{D}_i$ is the disk whose center is at $\mathscr{C}_i$ and whose radius is d_u. The dependency of the coverage degrees of points $\mathscr{C}_1$ and $\mathscr{C}_2$ is represented by the intersection of the two disks.

To investigate the dependency of the coverage degrees, we have to first look into the deployment probabilities of the crescent areas $\mathscr{A}_1$ and $\mathscr{A}_2$, and the intersection area $\mathscr{A}_3$ which are defined as:

$$\mathscr{A}_3 = \mathscr{D}_1 \cap \mathscr{D}_2, \quad \mathscr{A}_i = \mathscr{D}_i - \mathscr{A}_3, \quad i = 1, 2.$$

Let the random variable $\mathscr{Y}_i$ denote the number of nodes that reside in $\mathscr{A}_i$. Then,

$$P(\mathscr{Y}_i + \mathscr{Y}_3 = n) = P(\mathscr{X}_i = n), \quad i = 1, 2, \tag{4}$$

where the random variable $\mathscr{X}_i$ denotes the number of sensor nodes that have non-zero detection probability, i.e. the sensor nodes that resides within the d_u-distance of the event point $\mathscr{C}_i$.

Given that point $\mathscr{C}_1$ has coverage degree c_1, the probability that point $\mathscr{C}_2$ has coverage degree c_2 is found as follows. Define $c_{\min} = \min(c_1, c_2)$. Then,

$$\begin{aligned} P(\mathscr{X}_2 = c_2 | \mathscr{X}_1 = c_1) \\ = \sum_{i=0}^{c_{\min}} P(\mathscr{X}_2 = c_2 | \mathscr{Y}_3 = i) P(\mathscr{Y}_3 = i | \mathscr{X}_1 = c_1). \end{aligned} \tag{5}$$

If it is known that there exist c_1 sensors on the first disk, then the probability of having i of them inside $\mathscr{A}_3$ possesses a Binomial distribution, where the probability of success is $\mathscr{A}_3/\pi d_u^2$. Hence,

$$P(\mathscr{Y}_3 = i | \mathscr{X}_1 = c_1) = \binom{c_1}{i} \left(\frac{\mathscr{A}_3}{\pi d_u^2}\right)^i \left(1 - \frac{\mathscr{A}_3}{\pi d_u^2}\right)^{c_1 - i}. \tag{6}$$

The probability of having $c_2 - i$ sensors within $\mathscr{A}_2$ again possesses the Binomial distribution. However, c_1 sensors are known to be out of that area. Hence, we are left with $N - c_1$ sensors to be deployed in the entire surveillance area minus $\mathscr{D}_1$. As a result,

$$\begin{aligned} &P(\mathscr{X}_2 = c_2 | \mathscr{Y}_3 = i) \\ &\quad = P(\mathscr{Y}_2 = c_2 - i) = \binom{N - c_1}{c_2 - i} \\ &\quad \times \left(\frac{\mathscr{A}_2}{LW - \pi d_u^2}\right)^{c_2 - i} \left(1 - \frac{\mathscr{A}_2}{LW - \pi d_u^2}\right)^{N - c_1 - (c_2 - i)}. \end{aligned} \tag{7}$$

Therefore, given c_1, the probability of having a coverage degree of c_2 in the next detection point can be calculated by using (5)–(7). However, according to (2), even if the coverage degree of a detection point is known, the number of target detections, and hence, the number of data packets generated are probabilistic. To calculate the detection degree of an event point, we first have to find the probability of event detection, $\varphi(d)$, per sensor node within the sensing range d_u. Then, a PMF for the number of detecting nodes can be generated which is a function of coverage degree $c_{x,y}$. For that, we utilize the *circle area element* definition which is illustrated in Fig. 4. The circle area element is defined as

$$dA = r dr d\theta.$$

Assume that a sensor node resides within the sensing range of the event location. Then, the probability of detection, γ, is equal to the probability that the sensor resides in any specific circle area element and detects the target from that distance. For any sensor within d_u distance of the target,

[3] The locations that the target resides at sampling times will be named *detection point* or *event point*, even if the detection degree is zero for the sake of readability.

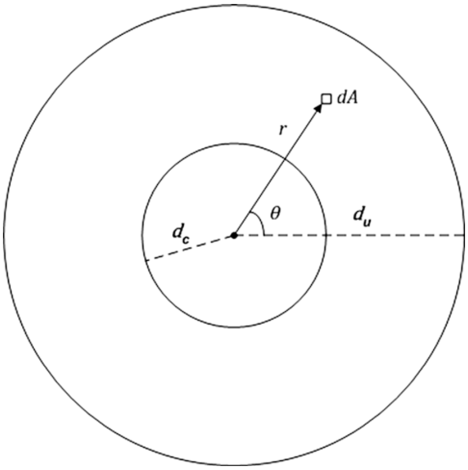


Fig. 4. Circle area element at distance r and with angle θ.

$$\gamma = \int_0^{2\pi}\int_0^{d_u}\frac{dA}{\pi d_u^2}\varphi(r) = \int_0^{2\pi}\int_0^{d_u}\frac{rdrd\theta}{\pi d_u^2}\varphi(r). \tag{8}$$

However, $\varphi(r)$ is a piecewise function and therefore the integral in (8) can be divided into appropriate intervals as in

$$\gamma = \int_0^{2\pi}\int_{d_c}^{d_u}\frac{rdrd\theta}{\pi d_u^2}e^{-\alpha(r-d_c)^\beta} + \int_0^{2\pi}\int_0^{d_c}\frac{rdrd\theta}{\pi d_u^2}. \tag{9}$$

Eq. (9) can be integrated according to the Elfes parameter values used. For $\beta = 1$, the probability of detection is found to be

$$\gamma = \frac{d_c^2}{d_u^2} + \frac{2}{\alpha^2 d_u^2}[1 + \alpha d_c - e^{\alpha(d_c-d_u)}(1 + \alpha d_u)]. \tag{10}$$

When all sensors are identical, which implies the same γ, and because sensor nodes are distributed uniformly, the PMF of the detection degree of the event point is Binomial with the probability of success, γ.

If we define $\mathscr{K}_i$ to be the random variable that represents the detection degree of the event point $\mathscr{C}_i$, then

$$P(\mathscr{K}_i = k_i|\mathscr{X}_i = c_i) = \binom{c_i}{k_i}\gamma^{k_i}(1-\gamma)^{c_i-k_i}. \tag{11}$$

The probabilities of possible detection degrees of a point can be calculated if the coverage degree of that point is known. However, as (5) indicates, the coverage degrees of successive detection points are not i.i.d., which means that the numbers of successive data packet generations are dependent. Given that $\mathscr{C}_j$ is the subsequent point of detection point that comes right after $\mathscr{C}_i$, and k_j is the detection degree of the detection point $\mathscr{C}_j$, this dependency can be formulated as

$$\begin{aligned} &P(\mathscr{K}_j = k_j|\mathscr{X}_i = c_i) \\ &\quad = \sum_{c_j=0}^{N-c_i} P(\mathscr{K}_j = k_j|\mathscr{X}_j = c_j)P(\mathscr{X}_j = c_j|\mathscr{X}_i = c_i). \end{aligned} \tag{12}$$

Table 1
Parameters for the reference scenario.

Parameter	Notation	Value
Border length	L	10,000 m
Border width	W	1000 m
Number of sensors	N	10,000
Sensing range	d_u	20 m
Certain detection range	d_c	0 m
Sensing parameter	α	0.1
Sensing parameter	β	1
Target velocity	v_T	10 m/s
Sensing interval	t_s	1 s

The accuracy of the analytical formulation derived for the components of SPTM framework is verified in Section 3. Moreover, the packet traffic generation using these formula is presented in Section 4.

3. Validation of SWSN packet traffic model (SPTM) framework

As a reference scenario, we set the system parameter values as specified in Table 1, and investigate the coverage and the detection degrees of the area points under uniformly distributed random deployment. The value for the parameter *Number of Sensors* is selected so that if regular grid deployment is employed, that many nodes are required for a minimum coverage of 99% of the surveillance area.

For evaluating the case with the Elfes detection model, 10,000 simulation runs are performed. At each run, N sensors are randomly deployed to a rectangle surveillance area that has length L and width W with uniform distribution. Then, one target crosses the area with the velocity v_T. While the target crosses the area, at each t_s seconds, the coverage degree of the target location and the number of target detections generated are logged with the corresponding time values to be able to extract the dependency of successive target locations. Detection of the target by the surrounding sensor nodes are determined probabilistically based on the sensor-target distance. The target uses the shortest crossing path.[4] As a result, at each simulation run, $\lfloor W/v_T t_s \rfloor = 100$ samples are taken in which the target is possibly detected. At each sampling, the coverage and detection degree values of the target locations are logged. After all simulations are completed, the probability mass functions are constructed based on the following histograms of the logged data:

- Histogram of the detection degrees observed, k_i, for the target detection points with coverage degree c_i, which is denoted as $Hist(k_i|\mathscr{X}_i = c_i)$,
- Histogram of the coverage degrees of the successor target detection points for the locations with coverage degree c_i, which is denoted as $Hist(c_{i+1}|\mathscr{X}_i = c_i)$.

[4] As will be described in Section 4, any target trajectory with varying direction and speed can be used as an input to generate successive coverage and detection degrees, analytically.

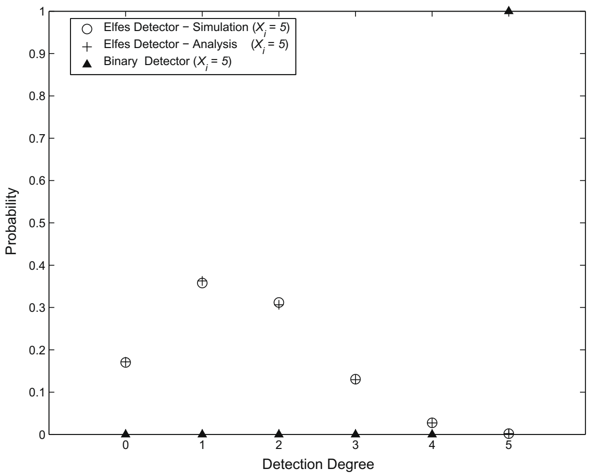


Fig. 5. The detection degree PMF for points with coverage degree of 5.

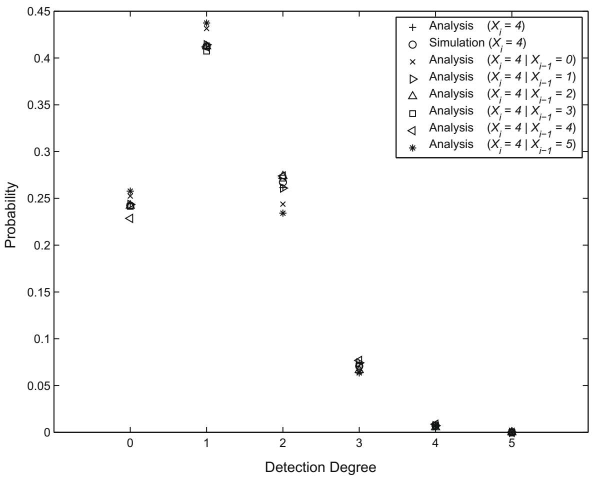


Fig. 6. The detection degree PMF for points with coverage degree of 4.

Fig. 5 depicts $P(\mathscr{K}_i = k|\mathscr{X}_i = 5)$, which is the detection degree PMF for the points with coverage degree of 5. As seen in the figure, the simulation results verify the analytical work presented for the probabilities of the number of sensors detecting an event, given the number of sensors within the sensing range. If the binary sensor detection model was used instead, the resulting PMF would give the probabilities of

$$P(\mathscr{K}_i = k|\mathscr{X}_i = 5) = \begin{cases} 1 & \text{if} \quad k = 5, \\ 0 & \text{otherwise}, \end{cases} \tag{13}$$

which have very diverse values since the number of sensor nodes within the sensing range of the target directly gives the number of sensors detecting this target, i.e. if a sensor is within the sensing range of the target, it detects the target with probability 1. To show that the detection degree PMF of an event point is determined by its coverage degree regardless of the history of coverage degree values, $P(\mathscr{K}_i = k|\mathscr{X}_i = 4)$ is compared to $P(\mathscr{K}_i = k|(\mathscr{X}_i = 4)(\mathscr{X}_{i-1} = j))$ in Fig. 6. As Figs. 5 and 6 show, the packet traffic model presented in Section 2 provides a mathematical framework for the packet traffic incurred by the SWSN.

To achieve accurate packet traffic model, Elfes parameters should be set according to the detection characteristics of the sensors deployed. Fig. 7 depicts the effect of different certain detection ranges on the number of detections for a point with coverage degree of 5 where the sensing range of the sensors is 20 m. The figure shows the crucial effect of the sensing properties of the sensors on the detection degree probabilities. Note that the binary detection model is achieved for the special case where the certain detection range parameter, d_c is equal to the sensing range parameter, d_u. As seen in Fig. 7, the packet traffic based on the parametric detection model will be very different from the one based on the idealized binary detection model.

The significance of setting the Elfes parameters accurately is also seen in Fig. 8 where the detection degrees

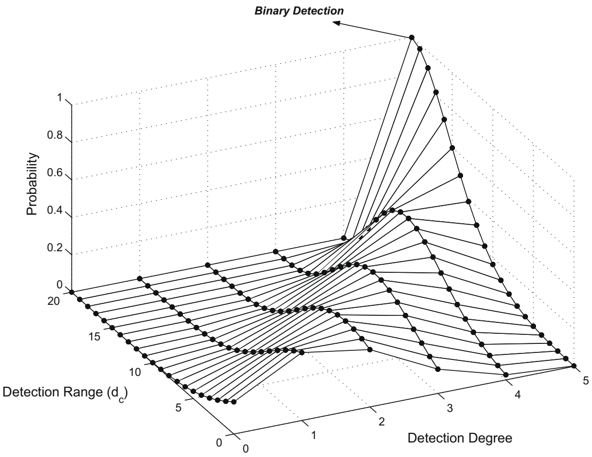


Fig. 7. The effect of the certain detection range parameter, d_c, on the detection degree probabilities for coverage degree of 5.

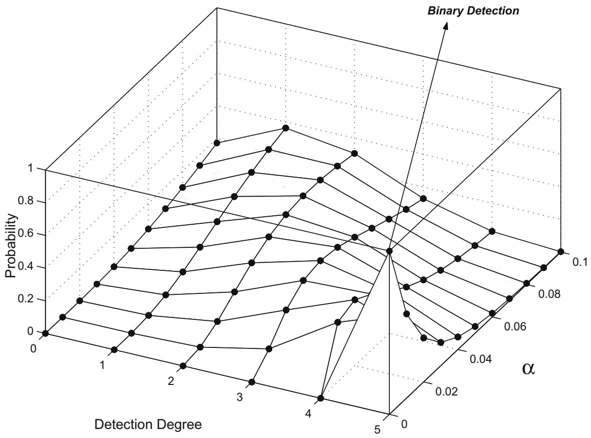


Fig. 8. The effect of the detection parameter α on the detection degree probabilities for coverage degree of 5.

for different values of the Elfes detection parameter α is shown. As the figure depicts, given a point with a specific coverage degree value, the detection degree probabilities varies considerably depending on the detection parameter value used. Hence, in addition to the use of a parametric detection model, the use of sensor-specific parameter values is also very crucial. Note that, setting the α parameter to zero yields the binary detection model which results in substantially different detection degree probabilities for a given coverage degree value.

4. Packet traffic generation using analytical SPTM model

Based on the presented analytical work for the coverage and the detection degree models, synthetic packet traffic for an intrusion detection scenario can be generated as follows.

4.1. SPTM packet traffic generation algorithm

Packet traffic starts with the entrance of the target to the surveillance area. Since there is no coverage degree history at that time, the initial coverage degree is generated according to the Poisson distribution with mean given in (3). Based on the detection degree PMF for the generated coverage degree value, a detection degree value is produced. Then, with the dependencies described in Section 2, subsequent coverage degrees and the corresponding detection degree values are generated. Algorithm 1 presents the steps to create sample packet traffic streams considering the Elfes detection model for $\beta = 1$ case.

Algorithm 1.

Packet traffic generation algorithm for the Elfes model

```
1: Set $c_0$ to be a random value chosen from the Poisson
   distribution with mean given in (3) {entrance point cov. deg.}
2: Calculate $\mathscr{A}_s$ based on the $v_T$, $t_s$ and $d_u$.
3: Calculate $k_0$ based on the probabilities found in (10)
   and (11) {entrance point detection deg.}
4: for $t = 1$ to $\left\lfloor \frac{W}{v_T t_s} \right\rfloor$ assuming a shortest crossing path do
5:     Choose a value for $c_t$ randomly, based on the
       probabilities found in (5)–(7).
6:     Calculate $k_t$ based on the probabilities found in (10)
       and (11).
7: end for
```

Although Algorithm 1 assumes a shortest crossing path for the target, any path with constant target speed can be evaluated by changing the second term in Step 4 with $\lfloor \ell / v_T t_s \rfloor$, where ℓ represents the length of the target crossing path. That is because all analytical work presented is still applicable by dividing the path into piecewise linear paths. In addition, if a target with varying speed and/or varying direction is to be simulated, the target trajectory can be used to generate the corresponding packet traffic as follows: Assume that the target trajectory is given as the vector $\mathbf{C} = [\mathscr{C}_1 \mathscr{C}_2 \cdots \mathscr{C}_\eta]^T$ where $\mathscr{C}_i$ stores the location of the target at ith sampling and η here represents the last sampling index before the target leaves the surveillance area. The modified algorithm that utilizes the target trajectory is given in Algorithm 2.

Algorithm 2.

Packet traffic generation algorithm for the Elfes model using a target trajectory

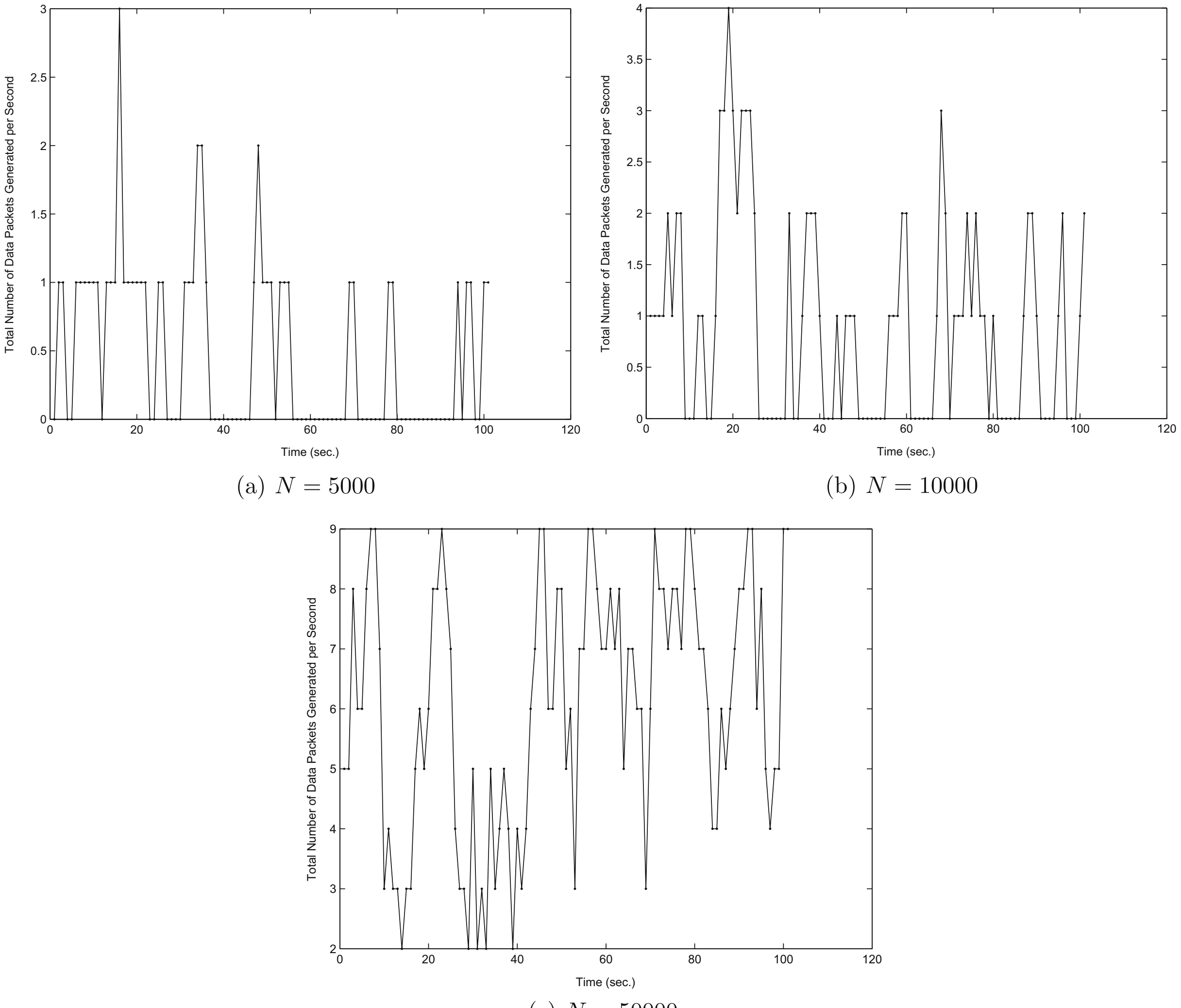
```
1: Set $c_0$ to be a random value chosen from the Poisson
   distribution with mean given in (3) {entrance point cov. deg}.
2: Calculate $\mathscr{A}_s$ based on the $v_T$, $t_s$ and $d_u$.
3: Calculate $k_0$ based on the probabilities found in (10)
   and (11) {entrance point detection deg.}
4: for $t = 1$ to $\eta$ {assuming a given target trajectory} do
5:     Choose a value for $c_t$ randomly, based on the
       probabilities found in (5)–(7) where $v_T t_s$ is replaced by
       the Euclidean distance between $\mathscr{C}_t$ and $\mathscr{C}_{t+1}$ in the area
       calculations.
6:     Calculate $k_t$ based on the probabilities found in (10)
       and (11).
7: end for
```

4.2. Traffic characteristics

Data traffic streams generated with Algorithm 1 are illustrated in Fig. 9 for varying number of sensor deployments, in other terms for varying sensor densities. If the target uses the shortest crossing path, then the path takes $\lfloor W/v_T \rfloor = 100$ seconds and the target is sensed for $\lfloor W/v_T t_s \rfloor = 100$ times by the sensors if $t_s = 1$ seconds. Fig. 9 depicts that the probability of target detection, and hence the data traffic rate increases as the sensor density increases as expected.

The effect of the target velocity is investigated in Fig. 10. As the target velocity decreases, the dependency between the successive number of data packet generations increases and the probability that similar number of data packets are generated at consecutive detections increases. However, as the target velocity increases, the PMF of the number of data packets generated approaches the *memoryless* Poisson distribution with the mean given in (3), which results in sharper changes in the number of data packets generated at consecutive detections.

The proposed packet traffic model enables the generation of sample data traffic streams or investigation of the effect of system parameter settings as illustrated in Figs. 9 and 10. To expose the characteristics of the three packet traffic models investigated, sample traffic traces with similar average traffic loads are shown in Fig. 11. The average load of the *periodic* packet traffic is adjusted by setting the data generation interval of the nodes whereas the average load of the *Binomial* packet traffic is adjusted by setting the data generation probability of the sensor nodes. For each traffic model, 50,000 nodes are deployed to the target area and the target average load is set to the one achieved with



(a) $N = 5000$

(b) $N = 10000$

(c) $N = 50000$

Fig. 9. Effect of node density on data traffic.

the SPTM traffic for the target speed of 1 m/s and the sensing range of 20 m. As seen in Fig. 11, the number of consecutive SPTM packet generations are correlated. That is why the interval of *the total number of packets generated per second* is larger in the periodic and Binomial packet traffic traces.

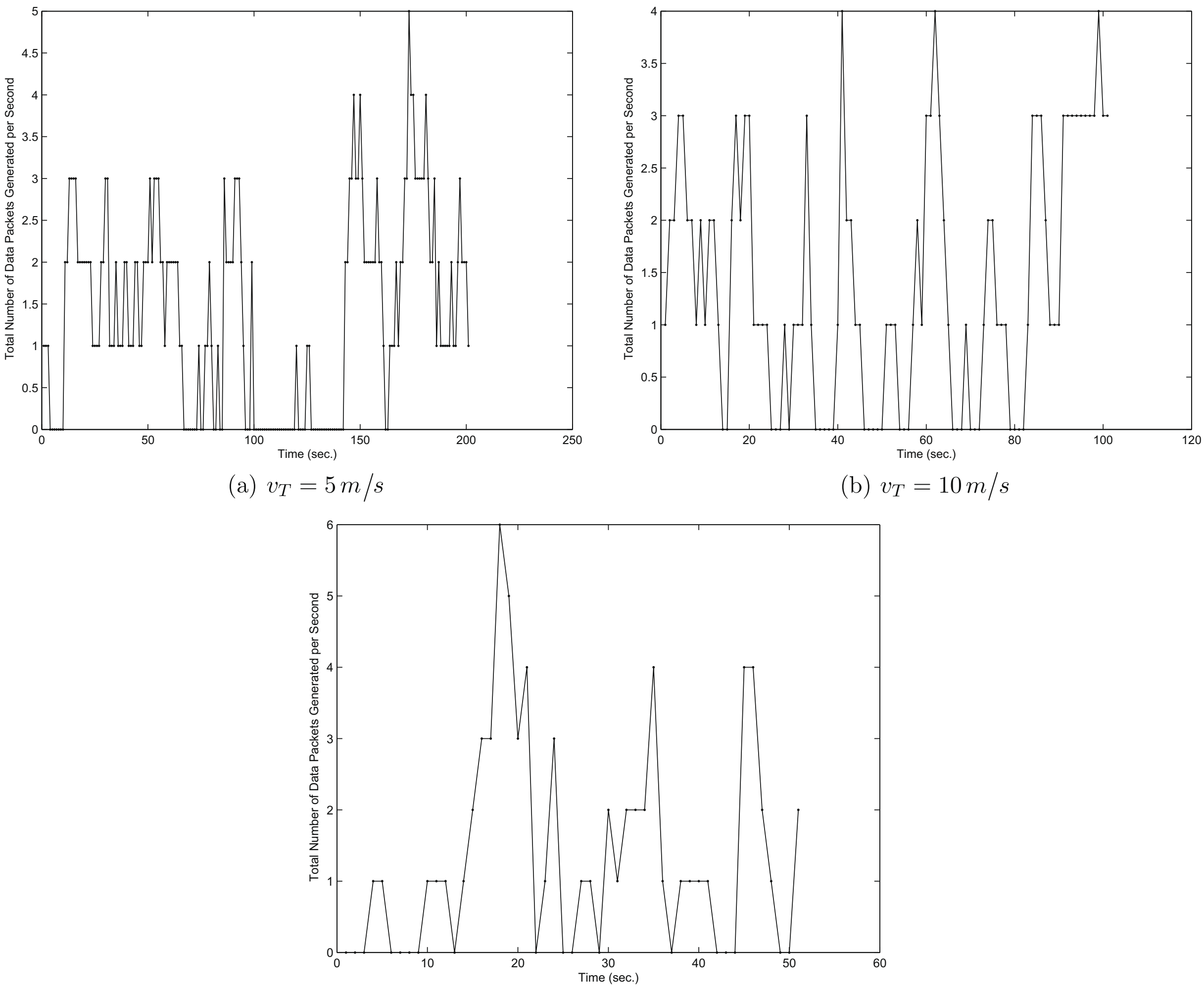
Although Figs. 9 and 10 show the traffic generated for shortest crossing paths, different target mobility models can be used in SPTM with Algorithm 2. The Gauss–Markov mobility model [21] is widely utilized in ad hoc networks where the speed and the direction of mobile node is assumed to be correlated over time and modeled as a Gauss–Markov stochastic process using the equations

$$\mathscr{S}_{t+1} = a\mathscr{S}_t + (1-a)\overline{\mathscr{S}} + \sqrt{(1-a^2)}\mathscr{S}_{X_t}, \tag{14}$$

$$\mathscr{E}_{t+1} = a\mathscr{E}_t + (1-a)\overline{\mathscr{E}} + \sqrt{(1-a^2)}\mathscr{E}_{X_t}, \tag{15}$$

where $\mathscr{S}_t$ and $\mathscr{E}_t$ are the new speed and direction of the target at time interval t; $\bar{\mathscr{S}}$ and $\overline{\mathscr{E}}$ are constants representing the mean value of speed and direction as $t \to \infty$, and $\mathscr{S}_{X_t}$ and $\mathscr{E}_{X_t}$ are zero-mean Gaussian distributed random variables. The degree of randomness is adjusted by the a parameter. As a increases, the current velocity is more likely to be influenced by the previous velocity, whereas setting a to zero yields the well-known Random Walk model. Fig. 12a shows a sample target trajectory for border crossing with mean speed of 10 m/s, mean direction of 90° (to represent the aim of crossing the border perpendicularly), the memory level parameter $a = 0.8$ and setting the Gaussian random variable variances to the one quarter of the mean speed and direction, respectively.

The packet traffic trace for the target trajectory shown in Fig. 12a is given in Fig. 12b. As seen in the figure, the consecutive packet traffic is correlated. This is an expected behavior since, for any target mobility model, the consecutive target detection locations will have similar coverage degrees. Gauss–Markov mobility model results in varying speeds, however when $v_T t_s < 2d_u$, the consecutive coverage degrees will be correlated. For $d_u = 20$ m and $t_s = 1$ s, the speeds below 40 m/s will result in a dependency,



(a) $v_T = 5\,m/s$

(b) $v_T = 10\,m/s$

(c) $v_T = 30\,m/s$

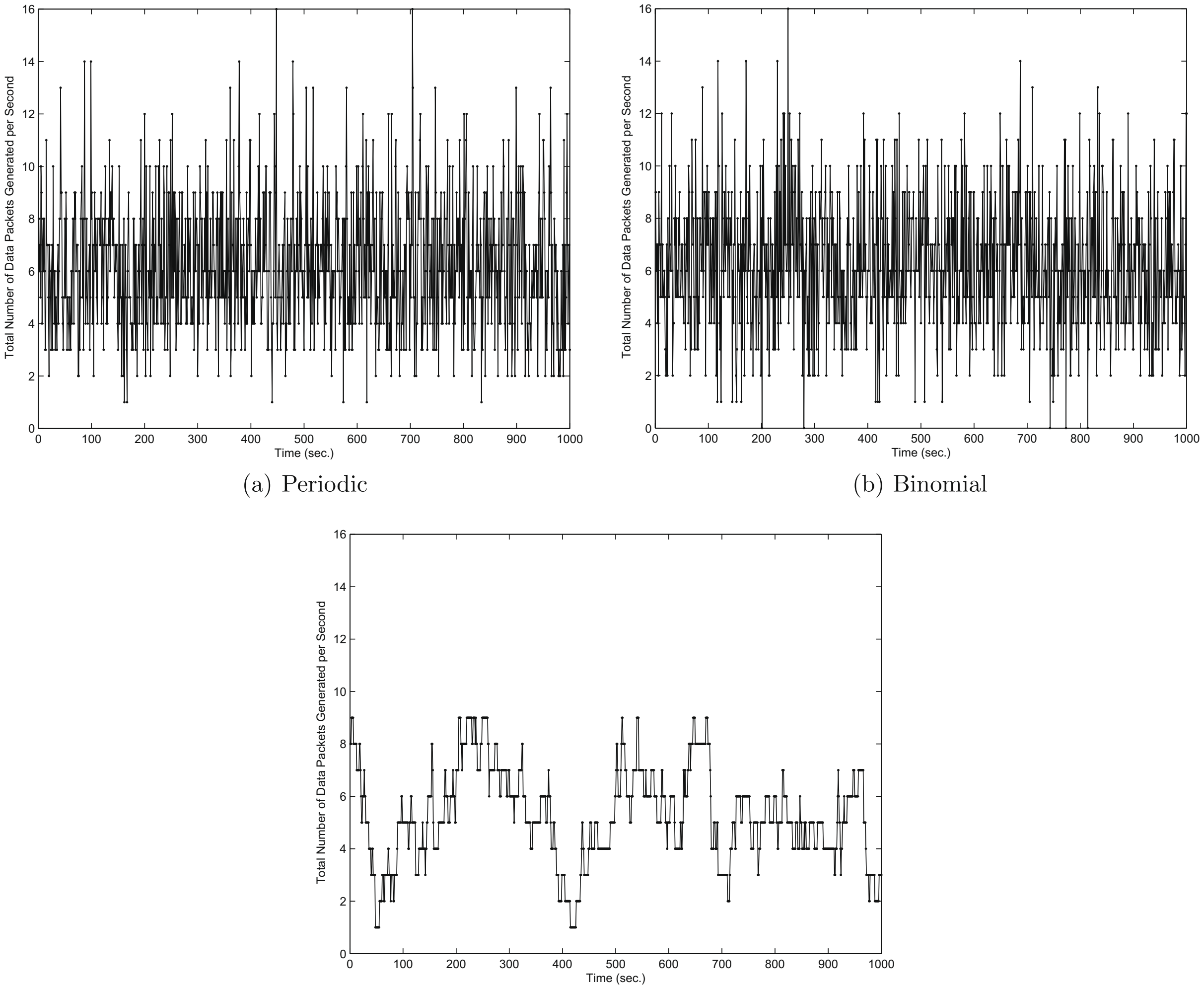
Fig. 10. Effect of target velocity on data traffic.

which actually corresponds to 144 km/h whereas the realistic target speeds are expected to be lower. For the rare cases where the target goes faster than 144 km/h, for the packet traffic creation, the Poisson distribution can be used to generate the coverage degrees and (8)–(11) can be used to generate the detection degrees based on these coverage degrees.

5. Impact of a realistic packet traffic model

To investigate the effect of the underlying packet traffic model, we conduct various simulations with three different types of packet traffic generation: (i) periodic data generation (ii) binomial data generation achieved by Bernoulli trials of the individual nodes, (iii) data generation by SPTM which corresponds to the realistic packet traffic for SWSN. We study the impact by examining the performance results for the Sensor-MAC (S-MAC) protocol [10]. S-MAC is a CSMA/CA-based MAC protocol that divides the network into virtual clusters, where the cluster members have the same sleep-listen schedules and the members at the intersection of different clusters also wake up at listen periods' of their neighboring clusters. Although there are a number of improvements on S-MAC such as Time-out-MAC (T-MAC) [22] and Dynamic Sensor-MAC (DSMAC) [23], because our goal is to show that using a realistic traffic model makes a difference, we will focus on the basic S-MAC protocol.

The performance of S-MAC is evaluated with the three different packet traffic models based on two performance criteria. The first one is the *average packet delay* as used in [24,25] which is a crucial performance metric for time-critical applications such as disaster monitoring and target tracking. For MAC protocols, packet delay is defined as the time passed from the data packet's reception by the sender's MAC layer to its arrival to the destination node's MAC layer which includes the queueing delay, collision delays and the transmission delay. Selecting the average packet delay as a performance metric also enables the



(a) Periodic

(b) Binomial

(c) SPTM

Fig. 11. Packet traffic traces of different traffic models with similar mean packet loads.

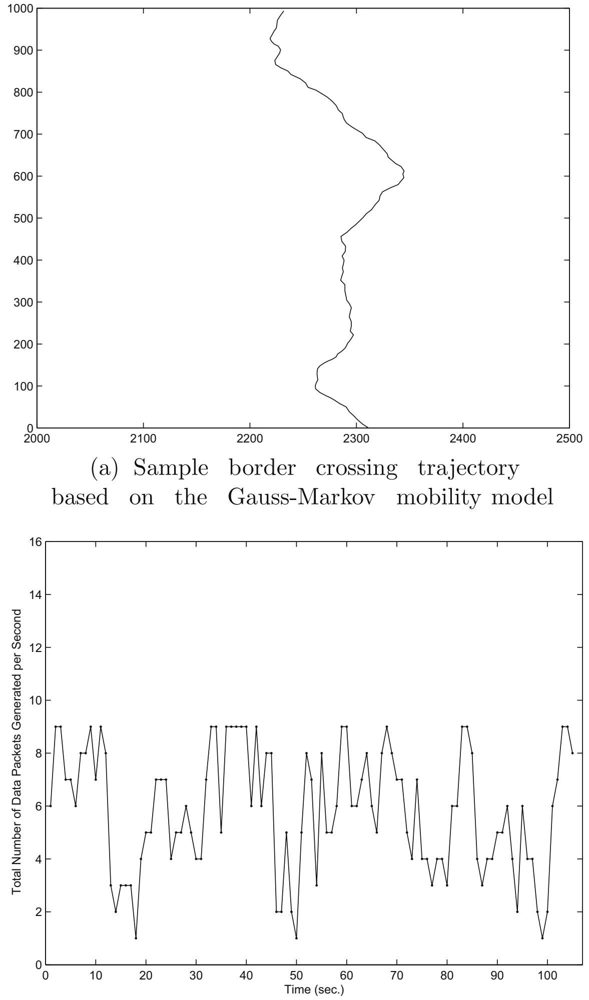
investigation of the maximum stable throughput of a system by inspecting the traffic load that results in infinite average delay.

The second performance criterion inspected is the *packet drop rate* as in [26,27], which is described as the rate of the packets dropped due to the limited buffer, or some other system or environment effect such as protocol time-outs. The packet drop rate is critical if the redundancy of the information sent is low, in other words if the information within each data packet is crucial for the application.

We consider one of the virtual clusters formed in the network separately to investigate the performance of the S-MAC protocol without the influence of the overlaying protocols such as the routing protocol. Within a virtual cluster, all members that have a data packet to send contend for the medium. S-MAC allocates contention slots for election of the node that will be given access to the medium. At the beginning of the contention slot period, all pending nodes pick a slot randomly. If a node did not receive start of any transmission before its slot's time arrives, it starts to transmit a ready-to-send (RTS) packet. Once the transmitted packet arrives at the destination node successfully, the destination node replies with a clear-to-send (CTS) packet. On the other hand, if the first occupied slot is actually selected by two or more nodes, then these nodes start transmitting their RTS packets at the same time, which results in a collision. These sender nodes realize the collision when no CTS packet is returned by the destination node within a specified time. Once the CTS packet is transmitted or the CTS time-out triggers, the contention slot procedure is started again. S-MAC simulation parameters and their values are listed in Table 2. Section 5.1 describes the three packet traffic patterns used in the simulations. Then, Section 5.2 presents the results of the comparison.

5.1. Packet traffic patterns

To evaluate the impact of the SPTM traffic pattern, two other data traffic patterns with different data traffic loads are used for comparison. The traffic load is defined as the



(a) Sample border crossing trajectory based on the Gauss-Markov mobility model

(b) Corresponding packet traffic trace

Fig. 12. SPTM traffic generation algorithm is used with Gauss–Markov mobility model.

Table 2
Scenario parameters.

Parameter	Value
Number of contending sensors	20
Bandwidth	20 Kbps
Data packet size	128 bit
RTS/CTS/ACK packet size	26 bit
Listen period	0.1 s
SYNC + Sleep period	0.9 s

number of new packet arrivals to a system, i.e. the total number of data packets created per unit time for WSN applications.[5] The periodic data traffic is achieved when each sensor node generates data with a specific time interval. A common interval is used by all sensors; however, they are allowed to choose a random offset. As a result, a periodically repeating packet traffic occurs. In this traffic model, average packet traffic load can be varied by changing the data generation interval defined in the system. To have a simplistic and non-periodic packet traffic, probabilistic data generation is used where the sensor nodes generate data packet at each unit time based on a specific probability. Consequently, the individual data traffic is a Bernoulli process and the aggregate data traffic becomes a Binomial traffic. Here, the traffic load is determined by the probability value assigned to all sensor nodes for data generation. Both periodic data traffic and Binomial packet traffic have the common property of being independent of external events such as target detection. Moreover, in both types of traffic, individual sensor data generation times are independent of the other sensors' data generations.

The SPTM traffic is composed of data packets generated by the sensor nodes at target detections. Hence, there is a dependency between data generations of the neighboring sensors which results in a bursty packet traffic. SPTM packet traffic scenario is generated as follows. Within the cluster area in which sensor nodes are deployed uniformly random, one target is assumed to move according to the random waypoint mobility model, which is commonly adopted in ad hoc networking research community [28,29]. In this model, the mobile is assigned a destination point ("waypoint") within the rectangular area defined, and a speed uniformly in a given interval. When it reaches the destination, it remains static for a predefined pause time and then starts moving again according to the same rule. With SPTM, different packet traffic loads are achieved by altering the value of the sensing range parameter of the detection degree model. The crucial parameters of the packet traffic scenarios and their value ranges used for the simulations are listed in Table 3.

Since we investigate the performance of the S-MAC and try to isolate it from the other communication layers, instead of simulating the whole border, we simulate just one part of it in which all nodes are one-hop away and are able to contend for the medium. Thus, we set a square shaped area in which all nodes can hear each other.

5.2. Packet traffic model simulation results

S-MAC is implemented in OPNET Modeler simulator [30] based on its ns-2 implementation [31]. Results presented in this section include the average delay and the packet drop rate of the S-MAC protocol for the three differ-

Table 3
Parameters of the packet traffic patterns.

Traffic type	Parameter	Value range
Periodic	Data generation interval	2.25–20 s
Binomial	Data generation probability	0.05–0.4
SPTM	Sensing range	15–40 m
SPTM	Target speed	1 m/s
SPTM	Pause time	0 s
SPTM	Area length	100 m
SPTM	Area width	100 m

[5] Two types of traffic loads are defined in the literature, namely, the *offered traffic load* and the *carried traffic load*. In this work, we study the changes in the system performance according to the number of data packets generated. Hence, we use the term *traffic load* to represent the *offered traffic load*.

ent packet traffic patterns under various average traffic loads. Each simulation run with a different seed generated a slightly different average aggregate load. Therefore, each simulation run is presented as a separate data point in the figures. The simulated network execution durations are limited to 12 h, which is sufficient for the convergence of the performance values and to have realistic performance results. For instance, within that duration, each sensor node generates approximately 2000 packets when periodic data traffic is selected with the packet interval parameter equal to 20 s.

5.2.1. Unlimited buffer case

The S-MAC performance results of one-hop delay averages are shown in Fig. 13 for different packet traffic patterns. As seen in the figure, except for very low data loads where no contention occurs and for very high data loads where the system is saturated, SPTM results in much higher delays than the binomial and periodic data traffic. The reason is that although the amount of data packets generated are close, the packet traffic generated by SPTM is bursty, which results in more contention compared to the other traffic types. Note that these delays are only one-hop link delays, and they must be accumulated until the data packet reaches the sink node for the calculation of the end-to-end delay. Hence, other traffic models overestimate the performance results of the S-MAC protocol for the SWSN applications, which may result in an inefficient system design.

The effect of the number of contending nodes on the performance results are investigated by comparing the three packet traffic types for 10, 20 and 30 nodes. Fig. 14 depicts the comparison where for all three cases SPTM packet traffic yields different performance results than the other two models. As the number of contending nodes increases, the average delays observed for a given load increase. The reason is that more contending nodes result in higher probability of collisions and hence, higher successful medium access delays.

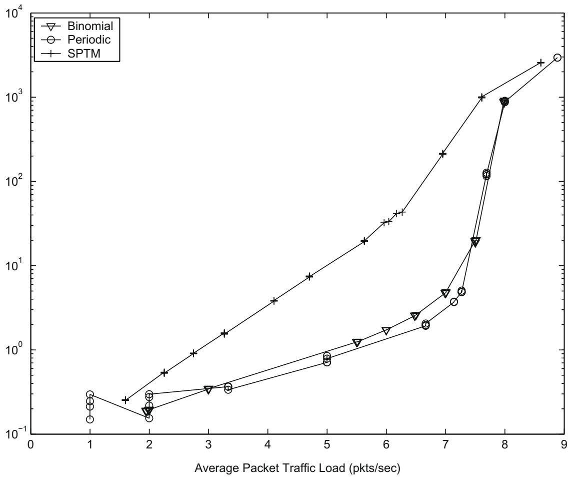


Fig. 13. Average delay vs. average load for the S-MAC protocol under different packet traffic patterns (log graph).

In addition to the average packet delays, we also explore the variance of the packet delays which can be important for the overlaying WSN application. We choose sample runs from each type of packet traffic pattern that has similar average traffic loads. Fig. 15 shows the delay histogram for the sample runs with the average data traffic load around 5 packets/s. The system is found to be stable in all of the traffic patterns under this average load. However, as seen in Fig. 15, for similar average traffic loads, the packets arrive with larger delays when SPTM pattern is used.

The SPTM scenario parameter settings also shape the MAC performance as shown in Fig. 16, where the average delay results for two different target velocities are shown. Hence, to have a realistic model, appropriate values of the system parameters should also be determined.

5.2.2. Limited buffer case

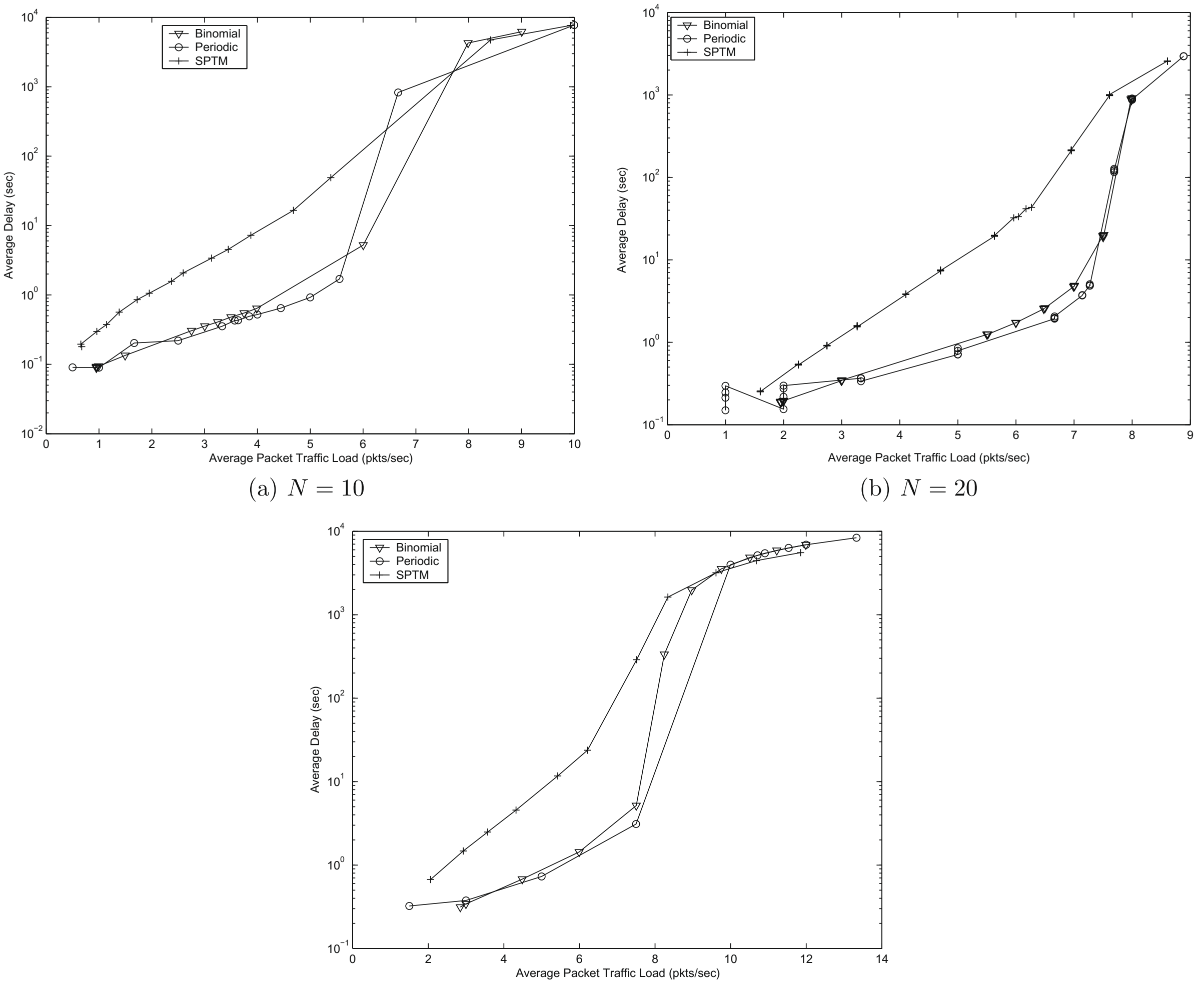
An important limitation in sensor nodes that should be considered is the limited memory capacity. That is why, in the real life scenarios, certain protocol limits are defined for the number of data packets to be buffered. In addition, if the delay of the packets in the queue reaches to a certain level, packet content can be useless for an application in which case the packet should be dropped. If a new data packet arrives from the application layer when the data buffer is full, either this packet can be merged to the previous packets by data aggregation, or one of the old packets or the new packet may be dropped. Since the packet drop rate is an important indicator for the MAC protocol performance, we study the limited buffer systems for this criterion, setting the data packet buffer limit to be 10 or 50 packets.

The packet drop percentages for different packet traffic patterns are shown in Figs. 17 and 18 for the buffer size of 10 and 50 packets, respectively. The SPTM resulted in much higher packet drop rates for the traffic loads higher than 3 and 5 packets/s, respectively. This is also an indication of burstiness of the packet traffic generated by the SPTM, since similar traffic loads always result in more packet drops for SPTM. Moreover, for the range of 3–7 packets/s, although there is no packet drops in the other traffic types, SPTM packet traffic results in non-negligible packet drop rates.

We investigate the average delay results for the three packet traffic patterns for the case where the newly created packets are dropped when the buffer is full. Assigning a packet drop rate threshold of 10%, Figs. 19 and 20 show the average packet delays encountered for the buffer size of 10 and 50 packets, respectively. The SPTM packet traffic still creates much higher average delays compared to the two other packet traffic patterns.

6. Analytical verification of the maximum throughput found by the SPTM packet traffic

The figures presented in Section 5 includes the performance results of the S-MAC communication protocol achieved by simulation for the three different packet traffic models. To verify these results in part, we investigate the



(a) $N = 10$

(b) $N = 20$

(c) $N = 30$

Fig. 14. Average delay vs. average load for the S-MAC protocol for different number of contending nodes (log graph).

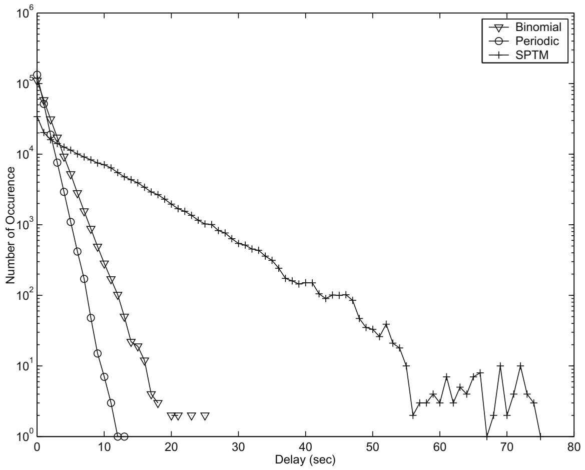


Fig. 15. Delay histogram of sample runs with similar average traffic loads.

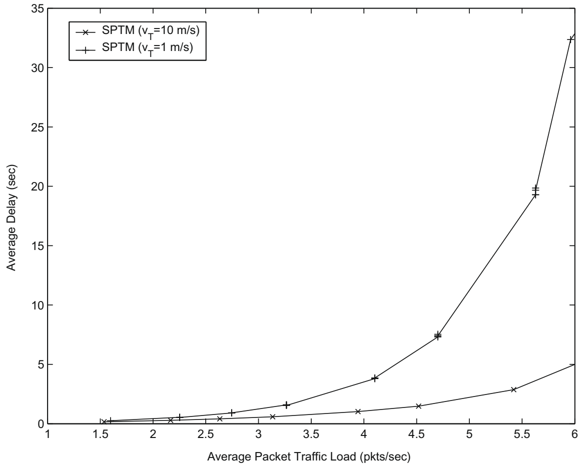


Fig. 16. Average delay vs. average load for the S-MAC protocol with different system parameter values.

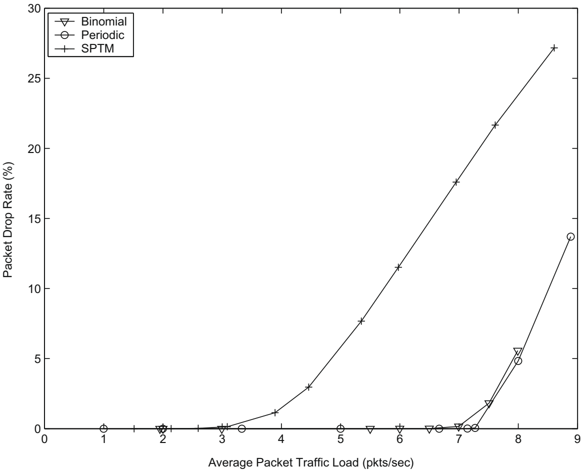


Fig. 17. Packet drop rate vs. average load for the S-MAC protocol with the buffer size of 10 packets.

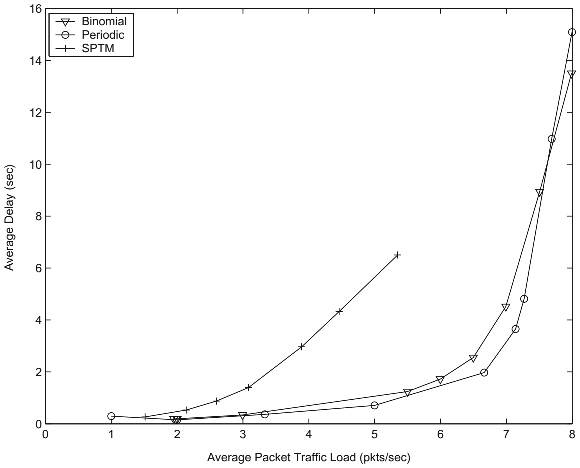


Fig. 19. Average delay vs. average load for the S-MAC protocol with allowable drop rates for the buffer size of 10 packets.

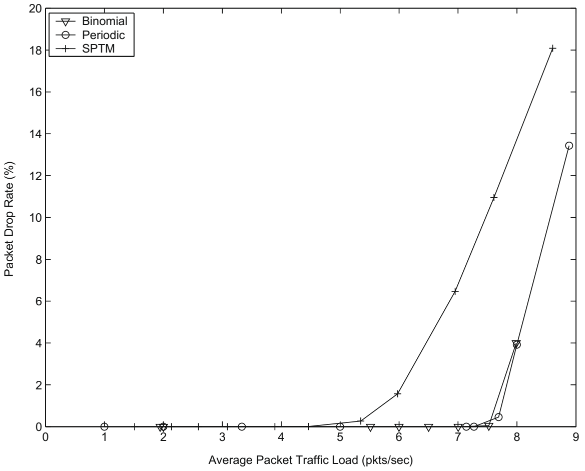


Fig. 18. Packet drop rate vs. average load for the S-MAC protocol with the buffer size of 50 packets.

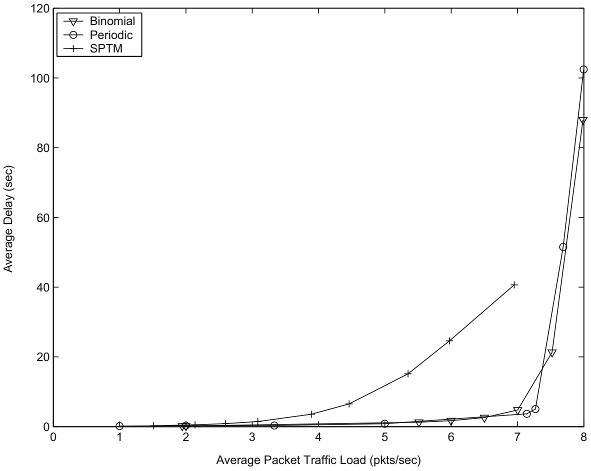


Fig. 20. Average delay vs. average load for the S-MAC protocol with allowable drop rates for the buffer size of 50 packets.

maximum stable throughput by analytical derivations and compare the outcome with the simulation results presented in Section 5.

In a multiple access system, offered load can be increased up to a certain point after which the system will be unstable, i.e. the expected delay will be unacceptable. This value will result in the maximum stable throughput. As the system approaches to an unstable point, every node will have data packets to send, and hence if there are $\mathscr{M}$ nodes within the investigated cluster, all $\mathscr{M}$ nodes will contend for the medium. However, for a MAC protocol, the maximum stable throughput is the maximum number of data packets that can be sent successfully per unit time in the steady state. Then for S-MAC, the maximum stable throughput, $\rho_{\max}$ is calculated as

$$\rho_{\max} = \frac{t_{\text{listen}}}{E[t_{\text{stx}}]}, \tag{16}$$

where t_{listen} is the listen period in seconds and t_{stx} is the time required for a successful packet transmission including the time lost with packet collisions and the duration of wait timers. Note that $\rho_{\max}$ has the unit *packets per listen-sleep period*. In (16), the expected value of the successful packet transmission time is used instead of the shortest feasible transmission time, since the steady state is considered when the maximum throughput is investigated.

S-MAC utilizes contention slots and RTS/CTS mechanism where the expected duration of a successful packet transmission is calculated as

$$E[t_{\text{stx}}] = E[t_{\text{coll}}] + E[t_{\text{CW}}] + t_{\text{RTS}} + t_{\text{CTS}} + t_{\text{DATA}} + t_{\text{ACK}}, \tag{17}$$

where t_{coll} represents the time spent for the collided packets' transmissions, t_{CW} represents the time spent for waiting the first occupied contention slot and all other t_X represent the time needed for the transmission of a packet of type X.

Since S-MAC is 1-persistent CSMA and collision is understood by the CTS time-out triggered when no CTS packet is received after t_{CTS}, the expected time spent for collisions is calculated as

$$E[t_{\mathrm{coll}}] = \sum_{z=0}^{\infty} z(E[t_{\mathrm{CW}}] + t_{\mathrm{RTS}} + t_{\mathrm{CTS}})\zeta^{z}, \tag{18}$$

where z is the number of successive collisions and ζ is the probability of packet collision in a contention period. However, in a protocol with contention slots, a collision occurs when the first occupied slot is selected by two or more nodes. Therefore, the probability that a slot assignment results in a collisionless transmission is

$$\xi = (1-\zeta) = \sum_{f=1}^{\mathscr{Z}-1} P(\mathscr{F} = f|\mathscr{Z},\mathscr{M}), \tag{19}$$

where $P(\mathscr{F} = f|\mathscr{Z},\mathscr{M})$ represents the probability that f is the first occupied slot and it is selected by only one node given that the contention window consists of $\mathscr{Z}$ contention slots and there are $\mathscr{M}$ contending nodes. Thus,

$$P(\mathscr{F} = f|\mathscr{Z},\mathscr{M}) = \frac{\mathscr{M}(\mathscr{Z}-f)^{\mathscr{M}-1}}{\mathscr{Z}^{\mathscr{M}}}, \tag{20}$$

because there are $\mathscr{Z}^{\mathscr{M}}$ different slot assignment possibilities among which the following assignments results in collisionless transmission: f is chosen by any of $\mathscr{M}$ nodes and the slots $f+1$ to $\mathscr{Z}$, i.e. $\mathscr{Z}-f$ slots, are chosen randomly by $\mathscr{M}-1$ nodes. Incorporating (20) into (21) yields

$$\begin{aligned}\xi &= \sum_{f=1}^{\mathscr{Z}-1} P(\mathscr{F} = f|\mathscr{Z},\mathscr{M}) \\ &= \mathscr{M}\frac{(2^{\mathscr{M}-1} + \cdots + (\mathscr{Z}-1)^{\mathscr{M}-1})}{\mathscr{Z}^{\mathscr{M}}}.\end{aligned} \tag{21}$$

The expected waiting time till the first occupied contention slot is

$$E[t_{\mathrm{CW}}] = \sum_{\psi=1}^{\mathscr{Z}} (\psi-1)P(\Psi=\psi)t_{\mathrm{slot}}, \tag{22}$$

where t_{slot} is one slot duration and Ψ represents the random variable of the index of the first occupied slot. Therefore, $P(\Psi=\psi)$ gives the probability that the ψth slot is the first occupied slot which can be defined as

$$P(\Psi=\psi) = P((s_i \geqslant \psi, \quad \forall i = 1..\mathscr{M}) \wedge (s_i = \psi, \quad \exists i = 1..\mathscr{M})),$$

where s_i represents the slot chosen by node i. Consequently,

$$P(\Psi=\psi) = \left(\frac{\mathscr{Z}-\psi+1}{\mathscr{Z}}\right)^{\mathscr{M}} - \left(\frac{\mathscr{Z}-\psi}{\mathscr{Z}}\right)^{\mathscr{M}}. \tag{23}$$

The maximum stable throughput of S-MAC under SPTM packet traffic can be calculated analytically once the system parameter values are given. To compare the maximum stable throughput achieved at simulation results with the analytically found throughput, the simulation parameters values given in Table 4 are applied to (16)–(23), and the maximum stable throughput formula components are calculated to be as tabulated in Table 5. According to these values, the maximum stable throughput is found to be 7.195 packets/s. The traffic load that results in instability in Fig. 13 matches the analytical maximum stable throughput result. Although the simulation results match the analytical results at the maximum stable throughput, the intermediate throughput-delay value calculations remain as an open issue.

Table 4
Simulation parameters used in analytical formula.

Parameter	Value
Number of contention slots	63
Number of contending nodes	20
Slot time	0.001 s
Sleep period	0.9 s
Listen period	0.1 s
Bandwidth	20 Kbps
Data packet size	128 bit
RTS/CTS/ACK packet size	26 bit

Table 5
Numerical results found by analysis.

Parameter	Calculated value
ξ	0.8492
ζ	0.1508
$E[t_{\mathrm{CW}}]$	0.0025 s
$E[t_{\mathrm{coll}}]$	0.0011 s
$E[t_{\mathrm{stx}}]$	0.0139 s

Note that these calculations require the exact average delay derivations for the given average traffic loads which must consider the randomly deployed node locations, randomly moving target's trajectory, MAC collision probabilities that depend on the number of data packets of the nodes and individual packet delays that depend on the packet queue size of the sensor nodes.

7. Conclusions

In this paper, a new packet traffic model framework is devised for intrusion detection applications using the Elfes sensor detection model. The system design parameters considered in this framework are the number of sensors deployed, the area size of the border, the detection distance thresholds, the target velocity, the sampling interval and the Elfes detection model parameters. Simulation results support the analytical work presented for the packet traffic model under this probabilistic detection model.

To show the importance of using a realistic packet traffic model for evaluating WSN communication protocols, we investigate the performance of S-MAC for different packet traffic models. Simulation results indicate that evaluating S-MAC with a packet traffic model other than the one proposed may give misleading results for the intrusion detection applications. The reason is revealed to be the bursty nature of the SPTM packet traffic which is proven analytically. Although, the effect of using a realistic packet traffic model is demonstrated for a MAC protocol, it can also be emphasized for other layers such as routing protocols. Moreover, the proposed model can be a baseline to have separate analytical studies for event-based WSN.

As a future work, the presented packet traffic model can be extended to include multiple target trajectories. In addition, the analytical traffic model can be updated by considering the relayed packets as part of the routing activity. The impact of using a realistic packet traffic model can also be investigated for the energy consumption metric. Using the proposed packet traffic model, the performance of various kinds of applications can easily be investigated such as the one in which the detecting nodes send their packets with a certain probability.

Acknowledgement

This work is supported by the Scientific and Technological Council of Turkey (TUBITAK) under the Grant Number 106E082.

References

[1] B. Gedik, L. Liu, P.S. Yu, ASAP: an adaptive sampling approach to data collection in sensor networks, IEEE Trans. Parallel Distrib. Syst. 18 (12) (2007) 1766–1783.

[2] S. Kashihara, N. Wakamiya, M. Murata, Implementation and evaluation of a synchronization-based data gathering scheme for sensor networks, in: Proc. IEEE ICC, vol. 5, Korea, 2005, pp. 3037–3043.

[3] S. Gandham, M. Dawande, R. Prakash, An integral flow-based energy-efficient routing algorithm for wireless sensor networks, in: Proc. IEEE WCNC, vol. 4, Atlanta, USA, 2004, pp. 2341–2346.

[4] Y. Ma, J.H. Aylor, System lifetime optimization for heterogeneous sensor networks with a hub-spoke topology, IEEE Trans. Mobile Comput. 3 (3) (2004) 286–294.

[5] X. Shi, G. Stromberg, SyncWUF: An ultra low-power MAC protocol for wireless sensor networks, IEEE Trans. Mobile Comput. 6 (1) (2007) 115–125.

[6] S.D. Muruganathan, A.O. Fapojuwo, A hybrid routing protocol for wireless sensor networks based on a two-level clustering hierarchy with enhanced energy efficiency, in: Wireless Communications and Networking Conference, 2008, WCNC 2008, IEEE, 2008, pp. 2051–2056.

[7] I. Demirkol, F. Alagöz, H. Deliç, C. Ersoy, Wireless sensor networks for intrusion detection: packet traffic modeling, IEEE Commun. Lett. 10 (1) (2006) 22–24.

[8] G.G. Messier, I.G. Finvers, Traffic models for medical wireless sensor networks, IEEE Commun. Lett. 11 (2007) 13–15.

[9] Y. Wong, W. Seah, L. Ngoh, W. Wong, Sensor traffic patterns in target tracking networks, in: Wireless Communications and Networking Conference, 2007, WCNC 2007, IEEE, 2007, pp. 4123–4126.

[10] W. Ye, J. Heidemann, D. Estrin, Medium access control with coordinated adaptive sleeping for wireless sensor networks, IEEE/ACM Trans. Netw. 12 (3) (2004) 493–506.

[11] Crossbow Technology Inc., MPR-MIB Users Manual, June 2006.

[12] Y. Zou, K. Chakrabarty, Sensor deployment and target localization based on virtual forces, in: Proc. IEEE INFOCOM'03, vol. 2, San Francisco, USA, 2003, pp. 1293–1303.

[13] Y. Zou, K. Chakrabarty, Uncertainty-aware and coverage-oriented deployment for sensor networks, J. Parallel Distrib. Comput. 64 (7) (2004) 788–798.

[14] A. Elfes, Occupancy grids: a stochastic spatial representation for active robot perception, in: S.S. Iyengar, A. Elfes (Eds.), Autonomous Mobile Robots: Perception, Mapping and Navigation, vol. 1, IEEE Computer Society Press, 1991, pp. 60–70.

[15] E. Onur, C. Ersoy, H. Deliç, How many sensors for an acceptable breach detection probability?, Comput Commun. 29 (2006) 173–182.

[16] E. Onur, C. Ersoy, H. Deliç, L. Akarun, Surveillance wireless sensor networks: deployment quality analysis, IEEE Netw. 21 (6) (2007) 48–53. November–December.

[17] W. Peng-Jun, Y. Chih-Wei, Coverage by randomly deployed wireless sensor networks, IEEE Trans. Inf. Theory 52 (6) (2006) 2658–2669.

[18] S. Ren, Q. Li, H. Wang, X. Chen, X. Zhang, Design and analysis of sensing scheduling algorithms under partial coverage for object detection in sensor networks, IEEE Trans. Parallel Distrib. Syst. 18 (3) (2007) 334–350.

[19] G. Wang, G. Cao, T.L. Porta, W. Zhang, Sensor relocation in mobile sensor networks, in: Proc. IEEE INFOCOM, vol. 4, Miami, USA, 2005, pp. 2302–2312.

[20] C. Pandana, K.J.R. Liu, Maximum connectivity and maximum lifetime energy-aware routing for wireless sensor networks, in: Proc. IEEE GLOBECOM'05, vol. 2, St. Louis, USA, 2005, pp. 1034–1038.

[21] B. Liang, Z.J. Haas, Predictive distance-based mobility management for PCS networks, in: INFOCOM (3), 1999, pp. 1377–1384.

[22] T.V. Dam, K. Langendoen, An adaptive energy-efficient MAC protocol for wireless sensor networks, in: Proc. ACM SenSys, Los Angeles, USA, 2003, pp. 171–180.

[23] P. Lin, C. Qiao, X. Wang, Medium access control with a dynamic duty cycle for sensor networks, in: Proc. IEEE WCNC, vol. 3, Atlanta, USA, 2004, pp. 1534–1539.

[24] J. Zhu, S. Papavassiliou, J. Yang, Adaptive localized QoS-constrained data aggregation and processing in distributed sensor networks, IEEE Trans. Parallel Distrib. Syst. 17 (9) (2006) 923–933.

[25] S.C. Ergen, P. Varaiya, PEDAMACS: power efficient and delay aware medium access protocol for sensor networks, IEEE Trans. Mobile Comput. 5 (7) (2006) 920–930.

[26] A.K. Karmokar, D.V. Djonin, V.K. Bhargava, Optimal and suboptimal packet scheduling over correlated time varying flat fading channels, IEEE Trans. Wireless Commun. 5 (2) (2006) 446–456.

[27] F. Zhenghua, L. Haiyun, P. Zerfos, S. Lu, L. Zhang, M. Gerla, The impact of multihop wireless channel on TCP performance, IEEE/ACM Trans. Netw. 4 (2) (2006) 209–221.

[28] C. Bettstetter, G. Resta, P. Santi, The node distribution of the random waypoint mobility model for wireless ad hoc networks, IEEE Trans. Mobile Comput. 2 (3) (2003) 257–269.

[29] L. Hu, D. Evans, Localization for mobile sensor networks, in: Proc. ACM MobiCom, Philadelphia, USA, 2004, pp. 45–57.

[30] Opnet Modeler, URL <http://www.opnet.com/products/modeler/home.html>, 2006.

[31] The Network Simulator-ns-2, URL <http://www.isi.edu/nsnam/ns/>, 2006.

Ilker Demirkol received the B.Sc. (with honors), M.Sc. and Ph.D. degrees in computer engineering from Bogazici University, Istanbul, Turkey, in 1998, 2002, and 2008 respectively. Currently, he is a post-doctoral researcher in University of Rochester, NY. He worked as a database, system and network engineer from 1997 to 2004. He was research and teaching assistant in Bogazici University, Computer Engineering department from 2004 to 2008. His research interests include the areas of wireless communications, wireless ad hoc and sensor networks, and optimization of communication networks.

Cem Ersoy received his BS and MS degrees in electrical engineering from Bogazici University, Istanbul, in 1984 and 1986, respectively. He worked as an R&D engineer in NETAS A.S. between 1984 and 1986. He received his Ph.D. in electrical engineering from Polytechnic University, Brooklyn, New York in 1992. Currently, he is a professor in the Computer Engineering Department of Bogazici University. His research interests include performance evaluation and topological design of communication networks, wireless communications and mobile applications. He is a Senior Member of IEEE.

Fatih Alagöz is currently an associate professor in the Department of Computer Engineering, Bogazici University, Turkey. He was with the Department of Electrical Engineering, Harran University, Turkey. During 2001–2003, he was with the Department of Electrical and Computer Engineering, UAE University, UAE. He obtained his D.Sc. degree in electrical engineering in 2000, from George Washington University, USA. His current research areas include terrestrial and satellite mobile networks, sensor networks, UWB communications. He has edited two books, and published more than fifty scholarly papers in selected journals and conferences.

Hakan Deliç received the B.S. degree (with honors) in electrical and electronics engineering from Bogazici University, Istanbul, Turkey, in 1988, and the M.S. and the Ph.D. degrees in electrical engineering from the University of Virginia, Charlottesville, in 1990 and 1992, respectively. He was a Research Associate with the University of Virginia Health Sciences Center from 1992 to 1994. In September 1994, he joined the University of Louisiana at Lafayette, where he was on the Faculty of the Department of Electrical and Computer Engineering until February 1996. He was a Visiting Associate Professor in the Department of Electrical and Computer Engineering, University of Minnesota, Minneapolis, during the 2001–2002 academic year. He is currently a professor of electrical and electronics engineering at Bogazici University, and a visiting professor with the Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology, Netherlands. His research interests lie in the areas of communications and signal processing with current focus on wireless multiple access, ultra-wideband communications, OFDM, robust systems, and sensor networks.