Modeling energy-efficient secure communications in multi-mode wireless mobile devices

Arcangelo Castiglione [a], Francesco Palmieri [b,*], Ugo Fiore [c], Aniello Castiglione [a], Alfredo De Santis [a]

[a] *Dipartimento di Informatica, Università degli Studi di Salerno, Via Giovanni Paolo II, 132, I-84084, Fisciano (SA), Italy*
[b] *Dipartimento di Ingegneria Industriale e dell'Informazione, Seconda Università di Napoli, Via Roma, 29, Aversa (CE), I-81031, Italy*
[c] *C. S. I., Università degli Studi di Napoli "Federico II", Via Cintia, 21, I-80126, Napoli (NA), Italy*

A B S T R A C T

Despite the wide deployment of advanced wireless coverage infrastructures, finding the best way for achieving secure mobile communication in every-day's life activities is still an open question. Indeed, a large number of mobile terminals, supporting multiple networking technologies, may be used to manage data from everywhere and at anytime. However, the effort required for achieving security, given the complexity of cryptographic algorithms, heavily affects the power consumption of terminals. Such energy demand, together with the one required to manage communication activities, makes energy-efficient secure communication among hardware-constrained handheld devices a challenging topic. In this work, we introduce an analytic energy model for secure communication among multi-mode terminals. This model describes the energy consumption of mobile terminals operating within a dynamic network scenario, considering both their interconnection and secure data exchange issues, in order to develop adaptive strategies for energy-efficient secure communications. Finally, the model has been validated through simulation.

1. Introduction

Because of the wide deployment of cellular networks and high capacity Wi-Fi coverage infrastructures, a large number of *Mobile Terminals (MTs)*, simultaneously supporting multiple networking technologies, may be used to store, access, manipulate, or communicate sensitive data from everywhere and at anytime. One of the main features of such MTs, is the support and inter-operation of multiple different mobile communication technologies, resulting into a heterogeneous multi-standard network coverage. In particular, when using multiple networking technologies opportunistically, each one supporting its specific security model, it is easy to note that ensuring content confidentiality and authentication becomes a real challenge. Furthermore, the computational efforts required for achieving security, due to the complexity of cryptographic algorithms, heavily affect the power consumption and consequently the energy demand of involved terminals, which are usually equipped with battery units of limited capacity, in order to contain their weight and size. Such energy demand, together with the amount of power required to manage communication activities carried out by using multiple network interfaces, makes energy-efficient secure communication among mobile hardware-constrained devices a non-trivial task.

* Corresponding author.
E-mail addresses: arccas@dia.unisa.it (A. Castiglione), francesco.palmieri@unina.it (F. Palmieri), ufiore@dia.unisa.it (U. Fiore), castiglione@acm.org (A. Castiglione), castiglione@ieee.org (A. Castiglione), ads@unisa.it (A. De Santis).

DOI: 10.1016/j.jcss.2014.12.022

Accordingly, in this work we studied the energy-related dynamics of secure communications among MTs providing multiple and heterogeneous networking capabilities. In particular, we formulate a comprehensive analytic energy model, which can be used to describe and estimate the energy consumption of MTs operating within a continuously evolving network scenario, by considering both communication and security-enforcement activities, mainly accomplished through cryptographic techniques. Each MT is both an information source and sink, hence needing to send and receive multiple messages in a secure manner from any other MT in the same network. Such a model, may be particularly useful for adaptively choosing the best option among multiple available ones, with the final goal of minimizing the overall energy consumption of involved terminals. The fundamental factors affecting energy-efficiency in secure wireless communications are analyzed carefully, in order to evaluate their joint effects on battery lifetime.

Therefore, the energy consumption estimation resulting from the proposed model, becomes an objective function that can be considered for evaluating or implementing power optimization strategies. In order to model, estimate and possibly predict the energy consumption for secure communications in multi-mode devices, we considered both the energy needed for pure network communication activities and the one associated to the operations ensuring end-to-end security.

In addition, in order to be as realistic as possible, we also considered a set of other factors, such as the motion of MT, the distance of an MT from the corresponding endpoint (in case of ad-hoc communications), either from the *Base Station (BS)* or from any other kind of *Access Point (AP)* (when operating in the more traditional infrastructure mode), as well as the signal quality and strength. In doing this, the proposed model also takes into account the effects on energy consumption associated to user mobility, and in particular to the authentication and re-authentication operations that MTs perform during their motion. In detail, for modeling energy consumption of cryptographic operations performed by a MT, we consider several factors, including the individual network interface activities, as well as how many end-to-end data exchange sessions are simultaneously active for each interface. Indeed, it is important to emphasize that the number of cryptographic operations performed is also strongly related to the involved MTs' "*mobility profiles*", which given a set of interacting users, describe their behavior in a specific period of time. Clearly, only by knowing in advance all the mobility patterns associated to such mobility profiles, we can estimate, for each session, the number of *authentications*, *key exchanges* and *key updates* performed. Accordingly, we model the fixed contribution of authentication, key exchange and key setup operations for each session, by taking into account the number of operations resulting from the above mentioned mobility patterns.

It is also necessary to point out that the proposed model is specifically targeted on secure end-to-end communication activities, thus it does not consider all the other energy-draining factors associated to MT equipment, along with operations such as flash storage access, display and backlight usage, operating-system specific burden, routing protocol overhead, etc.

The proposed model has been validated through simulation, by comparing the obtained results with power consumption data available in the literature. The comparison confirmed that the basic concepts and assumptions underlying our proposal are correct, as well as the associated ideas are promising and worth to be exploited by future works.

This paper is structured as follows. Section 2 provides an overview of the most popular systems/solutions for modeling energy consumption in several networking scenarios. Section 3 defines and evaluates what are the factors that most influence the energy consumption required by secure communications. Section 4 describes the energy-efficient secure communication model, which is the main focus of this work. Section 5 shows the results obtained by analyzing the model through simulation and finally, Section 6 presents some conclusions and possible future developments.

2. Related work

Due to the ever-increasing diffusion of handheld devices with limited hardware and software characteristics, the problem of *energy-efficiency* is gaining importance, both from the academic and industrial point of view. In recent years, there have been many research efforts aiming at modeling energy consumption of such devices, by considering either communications or operations perspectives, but always in a separate way.

Two of the most relevant works in MTs' energy modeling were proposed in [1,2]. In particular, [1] describes several experiments carried out to obtain detailed energy consumption measurements of IEEE 802.11 wireless network interfaces, when operating in an ad-hoc networking environment. In [2], instead, a model for evaluating the energy consumption of ad-hoc networks is presented. Several other contributions concerning energy modeling in *Wireless Sensor Networks (WSN)* are available in the literature.

In [3], a three-tier architecture for collecting sensor data in sparse WSNs, which achieves substantial power savings from energy-awareness practices, has been defined and analyzed. Moreover, such work defines a simple analytic model for evaluating performance when system parameters are scaled.

Furthermore, [4] presents a scalable simulation environment for WSN, providing an accurate per-node energy consumption estimation. The work presented in [5], instead investigates the problem of irregular energy consumption in a large class of many-to-one WSNs. In detail, it proposes an analytic model addressing this problem, which may be helpful for understanding the relevance of different factors on energy consumption rates.

Other research efforts focus on modeling energy consumption of handheld devices. The most notable of them is the one proposed in [6], which evaluates the energy consumption characteristics of three widespread mobile networking technologies, namely 3G, GSM, and Wi-Fi. Such work points out that 3G and GSM require a high *tail energy* overhead, because of lingering in high power modes after completing a transfer. Based on these considerations, it models the energy consumption

associated to the network activity for each technology, and accordingly, defines a protocol that is able to reduce the energy consumption of most common mobile applications.

Deterministic power modeling techniques have been used for studying the energy consumption in Wi-Fi [7], 3G [8], and LTE [9].

The first effort that combines into a single model the energy demands arising from both networking activities and cryptographic operations needed to implement secure sessions, has been presented in [10], where the architecture of an energy-aware framework for secure end-to-end communication among ubiquitous MTs, providing multiple and heterogeneous wireless networking capabilities is sketched. This work extends the aforementioned experience, by mainly focusing on the formulation of an analytic energy model that may be used to describe the energy consumption of multi-mode MTs operating within a cellular or WLAN radio coverage, by considering both network communication and security activities. Such a model, may be extremely useful for adaptively choosing the best option among multiple available ones, with the final goal of minimizing the overall energy consumption of involved devices, thus increasing their lifetime. In other words, the energy consumption estimation resulting from the proposed model, becomes an objective function that can be considered for evaluating or implementing power optimization strategies. The motivation behind such proposal, is to provide enhanced data transfer facilities while reducing the frequency of battery recharges. This improves the possibility to support secure communications involving massive data transfers, also in a hardware-constrained mobile environment.

3. Energy efficient secure communication for multi-mode devices

One of the main drawbacks in mobile technology is energy efficiency. In fact, MTs are affected by the problem that their batteries need to be regularly recharged from a power source and this obviously limits the lifetime of data transfer sessions. Furthermore, due to the obvious dimensional constraints characterizing, for practical reasons, almost all the state-of-the-art MTs, the energy source on such devices is only a (very) small battery, forcing them to rely on an extremely small power budget. For this reason, nowadays many research efforts in the fields of energy efficiency and power management focus their attention on battery-powered portable computers and mobile devices [11–16]. In the current section, we examine at a glance the components and factors which mostly affect the energy consumption of secure communications among multi-mode devices. In particular, we analyze how securing a session through cryptographic methods, between MTs equipped with multiple network interfaces, influences their overall power consumption.

3.1. Communication energy consumption

As the number of network interfaces and communication capabilities (e.g. *UMTS*, *LTE*, *IEEE 802.11b/g/n* and *Bluetooth*) available on MTs increases, manufactures have to face a huge (and critical) growth of the associated energy demand, which directly affects their functionality and usability. Indeed, communication is the most energy-draining task performed by MTs [17,6,18], so it is necessary to carefully manage the available network interfaces in order to minimize the overall power consumption of the whole communication. Approximately, 80% of power consumed by each MT is used for data transmission on communication channels [6]. In detail, MTs are connected to radio access subsystems, which may be considered as “legacy” network nodes, where mobile traffic originates and terminates. The radio access subsystem, typically consists of either an IEEE 802.11 Access Point in extended WLAN topologies or UMTS/LTE Radio Access network elements in the cellular or WWAN scenario. An MT usually may have multiple network interfaces, each characterized by an antenna and a power amplifier. In particular, such amplifier is the component with the highest impact on the overall power consumption. Therefore, according to the aforementioned considerations, the power consumption of a MT may be split into two distinct components:

- a fixed one, based on specific hardware and software characteristics, such as equipment and configuration in terms of network interfaces, their operating mode, transmission power, coverage range, etc.,
- a variable one, characterized by an energy-proportional demand profile, which varies over time depending on the current node activities.

More specifically, modern network interfaces are able to dynamically switch their operating modes, by passing through different power modes, characterized by different activities and processing capacities, as well as by different levels of power absorption. Thus, each wireless network interface, requires a fixed amount of energy to “stay operational”. In particular, such amount of energy (measured in *Joule* (J)/*second* (s) = *Watt* (W)), is independent from any transmission activity and is only used to keep the network interface powered-on and ready for communication. When an interface is not active, it may be put into *Sleep mode*. However, also in this case, the interface consumes a fixed amount of power, although significantly lower than the one required when the interface is active. In addition to such fixed consumptions, depending on the time during which the interface is “kept up”, the energy required for a data transfer is also characterized by consumptions which proportionally vary with respect to the transmission time, as well as to the amount of transmitted data (measured in μJ/bit or, equivalently, in W/Gbps). The overall energy drained by the transmission layer is hence given by the sum of fixed and variable energy consumptions of all its network interfaces, subject to the current communication burden. The energy profiles of interfaces associated to the various networking technologies may be quite different. For example, Wi-Fi interfaces

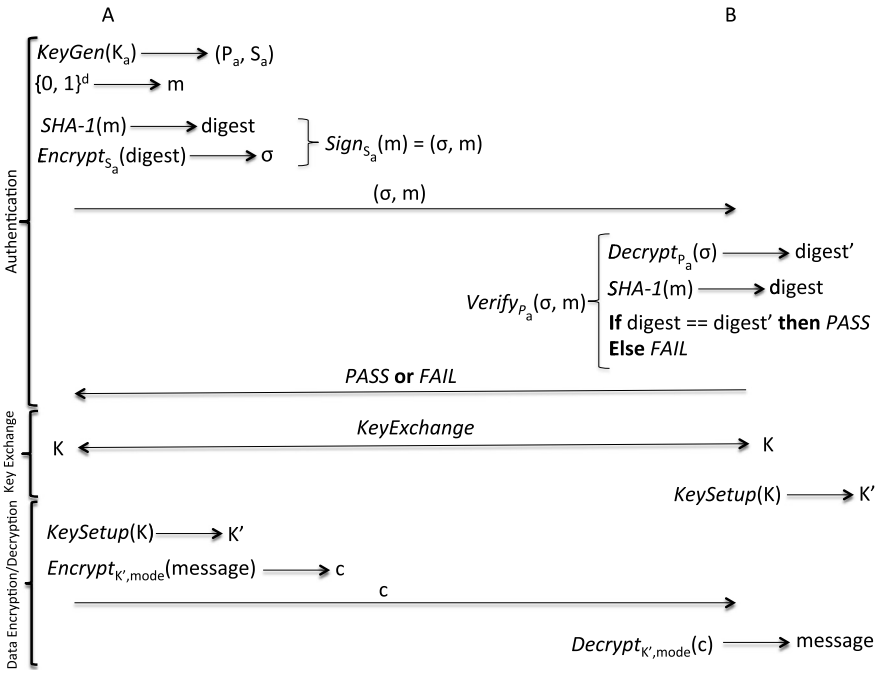


Fig. 1. Setting-up a secure session between multi-mode MTs.

require less energy than cellular ones for actual data transmission, but more energy to just keep the connection active [19]. In particular, it has been shown that transmission energy in Wi-Fi communications grows about three times slower than the cellular ones. On the other hand, GSM requires about 40% to 70% less energy than 3G, since its radio subsystem drains considerably lower power and presents a much shorter *tail interval* [6]. According to these considerations, Wi-Fi interfaces should be always preferred against 3G/2G ones. It has been observed [20] that, in both 2G/3G and Wi-Fi communications, energy consumed *per bit* drops as packet size increases, while energy consumed *per second* shows an approximately linear trend with respect to packet size. It is important to point out, that since the energy required per bit essentially depends on the packet size, an estimate of the energy dissipation based on the breakdown of consumption in a fixed part, independent of the bits to be transmitted, and a variable one, proportional to them, would crucially depend on the distribution of packet sizes. Although analyzing some commonly adopted distributions may be a meaningful alternative [21], estimating the energy consumption with respect to the time spent in each operating mode, is instead more realistic and stable.

3.2. Encryption energy consumption

In general, to ensure security during the interaction between two (or more) endpoints and to provide integrity of exchanged data, cryptographic algorithms are used. Typically, such algorithms fall into two main classes, denoted by *private-key cryptography* and *public-key cryptography*, respectively. In detail, algorithms belonging to the former class, use the same key for encryption and decryption operations, hence both endpoints need to share a common secret. Instead, algorithms belonging to the latter class, use different keys, respectively known as *public* and *private* keys. It has been shown in [22], that private-key techniques are almost 1000 times faster than public-key ones, because the latter require much more processing (and battery) power. Therefore, it is important to remark that public-key techniques should be used only when their tasks cannot be accomplished otherwise. Consequently, in order to ensure the best trade-off between security and power consumption, a sort of "*Hybrid Approach*", relying on the use of a combination of both techniques, is required. In general, during a typical secure session, after the preliminary authentication phase in which MTs trust each other, a key exchange operation is carried out, enabling endpoints to agree on a common key. Subsequently, by using such key, the session is secured through private-key techniques, usually by means of *block ciphers*. Fig. 1 shows all the steps required in a typical secure session, namely, authentication, key exchange and encryption. In detail, if the authentication phase is successful, the involved endpoints are able to perform the key exchange in order to agree on a common key. Finally, after the choice of the block cipher to be used, both endpoints carry out the key setup phase, in order to generate session keys suited for the chosen cipher. From now on, the communication between endpoints is performed securely.

It is important to emphasize that by properly choosing the "*optimal*" combination of techniques belonging to the aforementioned classes, it is possible to achieve secure and reliable communications, at the expanse of the lowest possible computational effort, thus ensuring the minimum energy consumption. Public-key cryptography is widely used for *mutual authentication* and *key exchange* operations. As instances for the proposed model, we evaluated *RSA* [23], *Digital Signature*

Algorithm (DSA) [24] and *Diffie–Hellman (DH)* [25], together with their elliptic-curves-based variants, namely, *ECDSA* [26] and *ECDH* [27]. On the other hand, private-key cryptography is mainly used for end-to-end *data encryption* and can be typically implemented through *block ciphers*. In detail, block ciphers perform encryption/decryption by passing data blocks to be secured through several iterations of a fixed sequence of operations, denoted as *rounds*. Such ciphers are typically characterized by three algorithms: *Encryption*, *Decryption* and *KeySetup*. The main parameters of a block cipher are: supported *key length*, *block size*, nominal *number of rounds* and *mode of operation*. More precisely, a block cipher can only transform (encrypt or decrypt) a fixed-length set of bits, denoted as *block*. Different modes of operation enable the transformation of amounts of data larger than a block by applying repeatedly, but according to different strategies, a single block cipher operation. As instances for the proposed model, we considered and evaluated the following block ciphers: *Rijndael* [28], *Serpent* [29], *RC6* [30], *Camellia* [31] and *Twofish* [32], together with the following modes of operation: *Electronic CodeBook* (*ECB*), *Cipher-Block Chaining* (*CBC*), *Cipher Feedback* (*CFB*), *Output Feedback* (*OFB*), *Counter* (CTR) and *Counter with CBC-MAC* (*CCM*). We made this choice because they are considered state-of-the-art cryptographically strong solutions. Finally, they are efficiently implemented for a large number of architectures and platforms.

4. An analytic energy model for secure communications

In order to formally describe the energy consumption of MTs, we propose a comprehensive analytic model, based on considerations made in Section 3. This model, is in line with the emerging trends characterizing energy-efficient devices and applications, which are able to dynamically adapt their behavior, depending on the current workload and the available networking technology coverage, in order to limit the overall associated energy consumption. The main aim of such analytic model, is to provide a comprehensive and unambiguous definition of MTs' energy consumption, by formalizing with a mathematical description their operating scenario, in order to allow the formulation of proper movement/communication strategies that are able to maximize MTs lifetime. In order to achieve a characterization of energy consumption that is as realistic as possible, we represent in a parametric way only the main functional aspects of a MT (communication and security technologies used), abstracting instead all the other less relevant details. In this way, the proposed model is virtually able to determine (and hence forecast) the energy consumption of involved devices, under any possible condition and for any possible operating scenario. Furthermore, since irrelevant hardware and software configuration details are totally abstracted or only partially represented, the proposed model is able to easily evolve and adapt itself, with respect to the state-of-the-art hardware equipment characterizing a device.

4.1. Modeling communication energy

MTs dynamically join and leave radio access coverage infrastructures, whose BS equipment (or relay nodes in ad-hoc scenarios) may be considered as legacy network gateways where mobile traffic originates and terminates. Clearly, such a model only focuses on energy consumption at the MT side, by not considering the energy impact on remote BSs. Specifically, the model is designed with the aim of ensuring flexibility and generality, through a sufficiently high abstraction degree in the characterization of the energy demand of MTs. Such demand depends at any moment on the current operational state of the network interface transmission circuitry. For the purposes of this work, we assume that energy consumption has to be evaluated by simultaneously taking into account four distinct operating modes, which are: *Transmit*, *Receive*, *Idle* and *Sleep*. In Transmit mode, the energy is drained by transmitting outbound packets, while in the Receive one, the energy is required for handling the reception of incoming ones. In order to proportionally reduce the consumption during inactivity periods, when the MT is silent and none is transmitting in its coverage range, it switches to Idle mode, thus requiring an amount of energy lower than in Receive mode. After passing a certain amount of time in Idle mode, without transmitting or receiving, the node is automatically switched into Sleep mode, where the radio component is put in a low energy demand mode, characterized by minimum power consumption, and immediately awakened when packets to be received or transmitted are available. It is important to remark that the radio circuitry may switch back to active (Transmit/Receive) mode in a reasonable time. At any given moment, an interface is in one mode only. For example, it cannot be transmitting and idle at the same time. In particular, we can model the overall network energy requirement (E_i) for a generic interface $i \in I_n$, of a MT n equipped with a set I_n of network interfaces, over a time period Δt, in two ways:

- representing its value as composed by the energy that it spends in each of its power modes, estimated by considering the instantaneous power consumption associated to each interface mode, along with the overall fraction of time spent in them;
- evaluating the expected value of E_i, considering an average instantaneous power consumption value in each mode, along with the probability distribution of the interface being in a given mode.

Such two estimations, respectively correspond to a deterministic and statistical approach, which may be used as alternatives for determining the basic model parameters. The driving idea behind the deterministic approach is mapping interface operations to communication activities and measuring (or estimating) the power required by the involved hardware components to carry out such activities. On the other hand, the statistical approach aims at determining relationships between power consumption and model variables, based on their probabilistic properties, such as distributions and mutual dependencies. In

the deterministic variant, the current operating mode must be known, e.g., the output of monitoring software operating on the MT. Moreover, the sampling period should be carefully chosen, in such a way that the power dissipation stays approximately constant over that period. However, the instantaneous transmit power depends on the channel condition, as well as on the distance between the MT and the other endpoint of the transmission link (note that this may be, and generally is, distinct from the other connection endpoint). Such distance may change over the time, as a consequence of smooth or sudden movements of the MT. Thus, it is questionable whether an estimation of the instantaneous power dissipation can be useful for the purpose of constructing a model of power consumption. Alternatively, from the statistical perspective, it is difficult to estimate the probability distribution of modes, since it depends on several factors, such as: node position with respect to its communicating counterpart, channel condition, along with intensity and direction of the data exchange. Also the transmission power output strongly depends on signal quality, which is in turn influenced by the environment. Quantity and direction of transmitted packets instead depend on the purpose and content of the communication itself. Therefore, expected values of the transmission parameters and movement patterns should be estimated over the considered time period.

Starting from the above considerations, we can deterministically model the energy demand $E_i(\Delta t)$ associated to the time interval Δt for the interface i characterized through a set of operating modes M_i, as composed by the energy that it spends in each of its power modes, by using Eq. (1), which considers the specific energy consumption characterizing each mode.

$$E_i(\Delta t) = \sum_{k \in M_i} E_i^{(k)}\left(\Delta t^{(k)}\right) = \sum_{k \in M_i} P_i^{(k)} \Delta t^{(k)}, \quad \text{with } i \in I_n \text{ and } \sum_{k \in M_i} \Delta t^{(k)} = \Delta t. \tag{1}$$

On the other hand, from the statistical-modeling point of view, it is important to remark that by considering the average energy dissipation over a time period Δt for a given number of MTs, the average $\bar{E}_i$ of E_i can be taken as an estimation of the expectation of E_i, and the same holds for each $k \in M_i$, as defined in Eq. (2):

$$\bar{E}_i(\Delta t) = \sum_{k \in M} \bar{E}_i^{(k)}(\Delta t) \cdot \bar{\tau}^{(k)}, \tag{2}$$

where $\bar{E}_i^{(k)}(\Delta t)$ denotes the average of energy dissipation in mode $k \in M_i$ during the time interval Δt and $\bar{\tau}^{(k)} \in [0, 1]$ is the average fraction of time Δt spent in that mode. In order to obtain a characterization of $\bar{\tau}^{(k)}$, the traffic in terms of arrival rate, the amount of data to be transmitted, and the transfer speed should be estimated, together with the average distance between endpoints, which introduces a further degree of complexity, thus making the deterministic modeling approach the best choice between the two available ones.

The energy required by interface i when it is respectively in Idle mode ($E_i^{(idl)}$) and Sleep mode ($E_i^{(s)}$), depends on the fixed idle ($P_i^{(idl)}$) and sleep ($P_i^{(s)}$) power absorption values associated to the interface hardware features, along with the overall time slices spent respectively in Sleep ($\Delta t^{(s)}$) and Idle ($\Delta t^{(idl)}$) modes. In addition, we define the transmit and receive energy demands by means of Eqs. (3) and (4):

$$E_i^{(x)}\left(\Delta t^{(x)}\right) = n_w^x \xi_w P_t + n_x \xi_b (P_x + P_o), \tag{3}$$

$$E_i^{(r)}\left(\Delta t^{(r)}\right) = n_w^r \rho_w P_t + n_r \rho_b P_r, \tag{4}$$

where P_x and P_r (measured in *Watts*) denote power consumptions of front-end components, respectively for transmitting and receiving activities, P_t represents the transition power, needed for switching to Transmit or Receive mode, and P_o denotes the output signal power (in *Watt*); ξ_b and ρ_b represent the time needed to send or receive a single bit of data (the bitrates); ξ_w and ρ_w denote the wake-up time of the circuit when entering in transmission and reception mode; n_x and n_r represent the number of bits respectively transmitted/received during time intervals $\Delta t^{(x)}$ and $\Delta t^{(r)}$. Finally, n_w^x and n_w^r represent the number of interface state transition to Transmit or Receive mode, respectively within the aggregated time slices $\Delta t^{(x)}$ and $\Delta t^{(r)}$. It is easy to note, that within a single continuous transmission interval, $n_w^x = 1$ and analogously, $n_w^r = 1$ in each single receive period. In addition, it holds that:

$$n_w^x \xi_w + n_x \xi_b \approx \Delta t^{(x)} \quad \text{and} \quad n_w^r \rho_w + n_r \rho_b \approx \Delta t^{(r)}. \tag{5}$$

For ease of exposition, we unify the wake-up times from the Sleep or Idle mode towards the Transmit or Receive ones, because the difference between them can be considered as meaningless. Analogously, we also considered the power needed for switching from Sleep mode to Idle as negligible. The transmission power output, denoted by P_o, may adaptively vary based on the distance D between transmitter and receiver, which may be either the other end-node, in ad-hoc communication scenarios, or the corresponding BS in infrastructured environments. In particular, P_o varies in order to be always at the minimum energy consumption level possible, while ensuring that the message is still correctly received by its intended destination. Therefore, in presence of adaptive transmission power output control, the current MT positions, influenced by the associated users' mobility profiles, assume a fundamental role when estimating communication energy consumption. Moreover, P_o depends on specific channel properties, such as the *gain* of involved transmitter (G_x) and receiver (G_r) antennas, receiver *power/sensitivity* (R_S) and the *radio frequency/wavelength* (λ). Formally, we model the transmission power output, varying upon distance and channel properties, according to Eq. (6) (Friis Equation).

$$P_o = \frac{R_S}{G_x G_r (\frac{\lambda}{4\pi D})^2}. \quad (6)$$

Despite its simplicity, the proposed model is general enough to consider also the effect of *tail energy* in GSM and UMTS/3G, due to the permanence in high-power modes after the completion of a transmission, as well as the association overhead in IEEE 802.11, by properly re-arranging the ξ_w, ρ_w and P_x parameters. In particular, by doing this, we reasonably assume that the effect of *ramp energy* (required for switching to a high-power mode before transmitting) on cellular transmissions is very limited and hence negligible. Furthermore, by relying on the "per-bit" transmit and receive power as its basic building block, the model naturally addresses implicit dependencies concerning the interface rate and the amount of data to be transmitted. The model may be also extended straightforwardly, to encompass cases in which a plurality of different Sleep modes is available, each with a different time required for switching back to active mode, and a power drawn which is inversely proportional, roughly, to that reactivation time.

The typical values that can be used as the basic model parameters have been empirically determined in [33–35] and fall within the ranges 0.6–1.4 W for Transmit mode, 0.3–0.9 W for Receive mode, 0.1–0.7 W for Idle mode and 0.01–0.05 W for Sleep mode, depending on the specific communication technology. Finally, given a MT n, its network energy consumption is characterized by Eq. (7):

$$E^n(\Delta t) = \sum_{i \in I_n} E_i(\Delta t), \quad (7)$$

where all the interfaces in I_n contribute to the overall energy demand. Since each MT n can simultaneously support different kinds of network interfaces, such as *IEEE 802.11*, *UMTS* or *GSM*, this model is able to represent the behavior of multi-mode MTs, choosing the best available networking technology at anytime. Given that the model essentially focuses on energy containment, the driving choice for the most suitable communication technology to be used at anytime is always the minimization of MT's energy consumption (*objective function*). For this reason, in presence of multiple coverages, the most energy-efficient technology among the available ones will be always selected. Thus, the per-interface energy demands E_i assume the role of weights that can drive the preference towards the best solution, minimizing the overall per-node energy consumption.

4.2. Modeling users' mobility profiles

The MT mobility profile plays a fundamental role in accurately estimating its energy consumption, and hence in determining the model effectiveness. Such profile may be considered as a tool which, given a set of interacting users, describes their moving behavior in a specific period of time. Therefore, it is substantially a facility which is able to model the behavior of a moving terminal among several endpoints. Such facility should be able to describe the moving patterns of MTs, resulting in the so-called "*mobility model*", whose operating variables must include MT location, speed and acceleration, besides how they vary over the time. Such information is necessary to reliably estimate the transmission power required by MTs, in particular when they perform secure communications while moving. Indeed, it is necessary for any communication model to consider the moving of target objects, which has to be carefully described in a simple but accurate and realistic way. Otherwise, any result/observation obtained by the involved model may be misleading. In order to be as realistic as possible, the modeling should also consider that the next-hop transmission termination may be another MT (also different by the communication endpoint), if operating in ad-hoc network communication scenarios, or a static BS when working in a more traditional infrastructure-based topology. However, in both of these cases, end-to-end communication takes place by passing through multiple relay steps, which may be either ad-hoc nodes or infrastructure components, occurring along the communication path between two communicating endpoints. Although a large number of complex mobility models is available for reliably describing MT mobility profiles (e.g., *Boundless Simulation*, *Gauss–Markov*, *Exponential Correlated*, *Column Mobility*, *Nomadic Community*, etc.) [36], the selection of an extremely sophisticated solution will not bring added value to our modeling task, since we are only interested in describing MT activities in terms of abstract mobility factors, representing the mobility patterns as external variables that only marginally affect our model. Accordingly, we considered for this purpose two of the most simple mobility models available: *Random Walk* and *Random Waypoint*. In the former, nodes move independently from each other, by randomly selecting a direction, an angle and a speed. The latter extends the former by introducing pause times between changes in speed and direction [36]. Nowadays, despite its simplicity, the *Random Waypoint* model is currently the reference (and most used) one in mobile communications scenarios. In such model, which we have chosen to manage mobility profiles, the operating scenario is bounded and obstacle-free, so that MTs mobility is not constrained. The moving behavior of MTs is extremely straightforward. In particular, each node, which is initialized at a specific position, randomly selects a destination point located anywhere in the moving scenario, together with a speed within a specific range, then it moves from its current position to the intended destination, according to a straight trajectory. Once the destination has been reached, the MT stays there for a uniformly distributed random amount of time, then it starts to move again, according to the same sequence of steps. Without loss of generality, the speed and direction of each MT are chosen independently from each other. In more detail, the *mobility factor* μ_i, may be considered as a measure characterizing the behavior of node i during a sample time interval Δt and may be modeled, as described in [37]. Formally,

$$\mu_i = \frac{1}{K\Delta t}\sum_{k=0}^{K-1}\left|A_i(k\Delta t) - A_i\big((k+1)\Delta t\big)\right| \quad \text{with } A_i(t) = \frac{1}{N-1}\sum_{j=1}^{N} D_{ij}(t), \tag{8}$$

where N is the total number of nodes in the network, $D_{ij}(t)$ is the distance between nodes i and j at time t, and $K = T/\Delta t$, with T being the total observation time.

4.3. Modeling encryption energy

By starting from the same deterministic modeling considerations that oriented the Section 4.1, for modeling energy consumption of cryptographic operations on a MT, we have taken into account several aspects, including its different processing capabilities, the available network interfaces, along with how many sessions are active for each interface. Obviously, for representing energy consumption in a realistic manner, we considered some form of dependency on the MTs mobility profile, which for simplicity has been modeled according to the aforementioned Random Waypoint model. Informally, we define a *session* as the interaction of an endpoint with another one, in order to exchange messages for any amount of time. For example, a session may be the interaction of user A with respect to B. By combining multiple individual sessions, the proposed model can describe both *end-to-end* and *one-to-many* relations between MTs. For each network interface of a MT n, we may have one or more sessions. Also in this case, for each session s, we model the energy consumption of cryptographic operations on a MT, denoted as $\mathcal{E}(s)$, by combining two factors: a fixed amount of power that does not depend on the data being transmitted, and a variable one, accounting for the energy-proportional behavior of modern hardware equipment, which increases with the traffic exchanged by the involved parties. The former fixed factor, depends on the key size and algorithms used for authentication, key exchange and key setup operations. The latter, can be influenced by a greater number of factors, such as the size (in bytes) of data payload p to be encrypted/decrypted, the block cipher $c_e(s)$ along with the involved mode of operation $m(s)$ (e.g., ECB, CBC, etc.), and the key size $k_e(s)$ of the cipher. In detail, for each session, we denote by $\gamma(k_a, c_a)$ the amount of energy required for the key generation (key setup) operation carried out by the authentication algorithm c_a, with key size k_a. Moreover, we denote by $\gamma(k_e, c_x)$ and $\gamma(k_e, c_e)$ the amounts of energy required for the same operation, performed by the key exchange algorithm c_x and by the block cipher c_e, both of them by using the same key size k_e. Finally, by using the same notation, we denote by $\sigma(k_a, c_a)$, $\upsilon(k_a, c_a)$ and $\chi(k_e, c_x)$ the fixed amounts of energy required for sign, verify and key exchange operations, carried out through algorithms c_a and c_x respectively, with their relative key size. We remark that the operations of signing and verification are required for the RSA-based strong mutual authentication. In order to model the energy consumption of cryptographic operations of a MT $i \in N$, we define the set $\Sigma_i(\Delta t)$, which denotes all the communication sessions involving node i active during the time interval Δt. Moreover, we define the variables $C^{(A)}$, $C^{(X)}$ and $C^{(S)}$, respectively denoting the energy consumption required for a single operation of authentication, key exchange and key setup, as explained earlier. Formally,

$$C^{(A)} = \gamma(k_a, c_a) + \sigma(k_a, c_a) + \upsilon(k_a, c_a), \qquad C^{(X)} = \gamma(k_e, c_x) + \chi(k_e, c_x), \qquad C^{(S)} = \gamma(k_e, c_e). \tag{9}$$

However, due to the motion of MTs and as a consequence of dynamics in the network context, the model needs also to consider how many times (statistically or in average) each of these operations is performed. Hence, based on what typically takes place in a real network scenario, we assume that the following conditions hold:

1. The authentication should be carried out each time a connection is established, either with a BS or with any other endpoint.
2. The key exchange can be performed one or more times, since the previously agreed key may be cached, expired or revoked.
3. The key setup can be done one or more times. Indeed, the involved endpoints may decide to change the block cipher to use, thus requiring a new key setup operation.

In order to estimate the energy consumption for each session s, we need to count the number of security operations (authentication, key exchange and key setup) that a determined endpoint performs with respect to another one. For this reason, we define the variables $R^{(A)}(s)$, $R^{(X)}(s)$ and $R^{(S)}(s)$, denoting the number of operations performed (per session) by a MT for authentication, key exchange and key setup, respectively. It is important to emphasize, that these variables are characterized by some form of dependency on the MT motion patterns, described by the chosen mobility model characterizing the MT behavior (in terms of movement) in relation to a given interface and network coverage. More precisely, by assuming that a session s is described by a pair of MTs (a, b), which represents the communication endpoints, we can model such a functional dependency as:

$$\big(R^{(A)}(s), R^{(X)}(s), R^{(S)}(s)\big) = f(\mu_a, \mu_b, I_a, I_b, \Delta t), \tag{10}$$

where μ_a and μ_b are the mobility factors of the involved endpoints, representing the average change of their distance to all the other nodes during a time interval Δt (the session duration), and I_a and I_b are their interfaces. It is easy to note, that due to the complex dependency of the function $f(\cdot)$ on several random factors and dynamics characterizing the mobility model, it cannot be expressed in an analytic way. Consequently, for each session s, the values of variables $R^{(A)}(s)$, $R^{(X)}(s)$

and $R^{(S)}(s)$ can be estimated only a posteriori (eventually through *discrete simulation*) starting from the mobility model together with the wireless communication model.

Therefore, the data-independent (fixed) contribution of authentication, key exchange and key setup operations for each session s, taking into account the mobility and communication patterns of the involved MTs, can be modeled through a parameter ϑ_s, formally defined by Eq. (11).

$$\vartheta_s = \left(C^{(A)} * R^{(A)}(s)\right) + \left(C^{(X)} * R^{(X)}(s)\right) + \left(C^{(S)} * R^{(S)}(s)\right). \tag{11}$$

On the other hand, the data-dependent part of energy consumption necessary to establish a secure session s, is proportional to the amount of data to be processed, denoted by p. In particular, it depends (*per session*) on the amount of energy needed for encrypting a single byte, denoted by $\varepsilon(c_e(s), k_e(s), m(s))$, which is based on several factors, such as the block cipher c_e, the key size k_e and the mode of operation m. It is easy to understand how the amount of data to be processed influences the energy consumption. Instead, it is not easy to appreciate the effect of the block cipher type, along with the associated mode of operation. Without going into technical details, the behavior of a block cipher may be viewed as a set of operations that transform a data understandable by all, into another one which is understandable only by those who have a proper secret key. Each of these operations is implemented at the machine level through a certain number of clock cycles, depending on the characteristics of the underlying hardware. Therefore, from the energy consumption standpoint, a block cipher differs from another one only by the number of clock cycles it requires for processing a single block of data. Obviously, the same holds for what concerns the relative mode of operation, which does nothing more than repeatedly applying a cipher's single-block operation, for transforming amounts of data larger than a block, thus affecting the block cipher consumption by a multiplicative factor. The energy values associated to the various encryption activities, modeled by functions $\varepsilon()$, $\gamma()$, $\sigma()$, $\upsilon()$ and $\chi()$, may be further determined by considering the specific CPU power-related features, along with the number of cycles needed to handle the cryptographic processing, which depend on both the cipher efficiency and the payload size. Each individual component $X \in \{\varepsilon(), \gamma(), \sigma(), \upsilon(), \chi()\}$, characterizing the energy consumption of a MT within a secure session, may be generically estimated, based on the implementation and technical specifications of the MT architecture, by using Eq. (12):

$$X = M_X \cdot Y \cdot F \cdot V^2, \tag{12}$$

where M_X is the number of machine instructions needed for the operation X, Y is the average number of CPU cycles for machine instruction, F is the CPU switching capacitance (measured in *Farads*) and V is its input voltage (in *Volts*). Clearly, the number of executed instructions/cycles grows with the algorithmic complexity of the associated security activity, leading to higher power consumption and energy demand. Therefore, we characterize the energy needed by cryptographic operations for each session s, through the sum of fixed and proportional energy consumption, as shown by Eq. (13).

$$\mathcal{E}(s) = \vartheta_s + p \cdot \varepsilon\left(c_e(s), k_e(s), m(s)\right). \tag{13}$$

Accordingly, the encryption energy consumption $\mathcal{E}_n(\Delta t)$ for the MT n during the time interval Δt is obtained by summing energy demands associated to each secure session $s \in \Sigma_n$ involving the MT n, as described by Eq. (14).

$$\mathcal{E}^n(\Delta t) = \sum_{s \in \Sigma_n(\Delta t)} \mathcal{E}(s). \tag{14}$$

In particular, in order to estimate the basic parameters for the proposed model, we considered the known power consumption values of several well-established security algorithms, reported in [38,39]. Moreover, we extended the results proposed in those works through interpolation, thus obtaining the estimated consumption parameters for all the aforementioned block ciphers, along with the relative modes of operation (see Table 1). In detail, we started by results that associate the number of clock cycles of some ciphers to the relative energy consumption. Subsequently, based on hardware specifications and machine instructions of the same processor from which the data described above has been obtained, we estimated the number of clock cycles of some other ciphers that have not been taken into account by the original sources [38,39], considering the operations they perform during their execution. In this way, we trivially estimated the consumption of such ciphers.

5. Experimental analysis

The behavior of the proposed model has been analyzed by using *discrete event simulation*, performed through the *NS-2 simulator* [40]. In all the simulation experiments, performed in an ad-hoc mobile wireless LAN scenario, the MTs have been modeled as homogeneous (i.e., with the same transmission range and interfaces, simulating the default *Lucent's WaveLAN IEEE 802.11b* card with an 11 Mb/sec bitrate), relying on a fully-shared wireless channel that can be accessed by any node at random times. The energy model parameters have been determined according to the measurement values reported in [34] and [6], for what concerns the communication aspects, as well as from [38,39] and Table 1 for all the encryption-related considerations. Several variable *Constant bitrate (CBR)* traffic loads, relying on *UDP* transport and multiple end-to-end connections, with up to 10 000 512-bytes messages sent on each connection, have been used in the analysis, within the context

Table 1
Energy required by the considered block ciphers.

Key size (bits)	Key setup (μJ)	ECB	CBC	CCM	OFB	CTR	CFB
Rijndael (μJ/Byte)							
128	7.83	1.21	1.65	1.91	1.62	1.53	1.61
192	7.87	1.42	2.08	2.30	1.83	1.72	1.80
256	9.92	1.64	2.29	2.31	2.05	1.93	2.01
RC6 (μJ/Byte)							
128	175	4.57	6.13	7.24	6.52	6	6.28
192	175.89	5.36	7.72	8.71	7.36	6.74	7.02
256	221.71	6.19	8.51	8.76	8.25	7.57	7.84
Serpent (μJ/Byte)							
128	19.6	4.10	5.50	6.49	5.50	5.20	5.45
192	19.7	4.81	7.06	7.81	6.21	5.84	6.09
256	24.8	5.55	7.77	7.84	6.96	6.55	6.80
Key size (bits)	Key setup (μJ)	ECB	CCM	CFB	OFB	CTR	CFB
Twofish (μJ/Byte)							
128	14.7	2.24	3.17	3.54	3.06	2.83	2.96
192	14.77	2.63	4.01	4.26	4.06	3.18	3.30
256	18.53	3.04	4.42	4.28	3.87	3.57	3.69
Camellia (μJ/Byte)							
128	42.84	3.66	4.90	5.74	5.14	4.75	4.82
192	43.06	4.29	6.29	6.91	5.80	5.34	5.39
256	54.28	4.95	6.92	6.94	6.50	6.00	6.02

of a *Random Waypoint* mobility model, in a square field of 1000×1000 m^2 and a pause time of 0 seconds, corresponding to continuous motion of MTs (with 20 m/s as maximum nodal speeds in some experiments and variable node speed in other ones). Each simulation was run for 500 seconds. *Unicast DSDV* routing with link layer support has been used to discover all the destination nodes solicited by the test traffic. End-to-end connection security is implemented through an initial RSA-based strong mutual authentication between involved endpoints, using a key size of 1024 bits, followed by a DH key negotiation which uses the same key size. In addition, all of the following messages are encrypted by using AES in ECB mode, with key size of 128 and 256 bits. All the basic choices and details describing the simulation scenario are summed up in Table 2.

In detail, several observations have been performed in three different scenarios, whose goal was to study how the energy drained in end-to-end secure communications is affected either by the prevailing network conditions, such as traffic load and node density, or by node mobility.

- In the first one, a single random mobile ad-hoc network consisting of 100 nodes has been solicited with several variable traffic loads, ranging from 10 up to 100 32-Kbps CBR connections, realized over end-to-end secure channels.
- In the second one, the network density has been varied from 60 up to 150 nodes, placed randomly on the aforementioned area, and solicited by using a fixed 32-Kbps CBR load of 50 secure connections.
- The last scenario explores the effect of a varying node speed (ranging from 0 up to 45 m/s), on a 50-nodes network solicited through a load characterized by 50 secure connections.

Overall, the observed values and trends acceptably match (i.e., proportionally, apart from some shift in scale associated to the use of different reference devices), with other well-established results presented in the literature, such as [41,42,20,43], thus validating the proposed model. We can also immediately observe from all the charts in Fig. 2 that the per-MT average energy consumed in Transmit mode is only a minor component of the total energy wasted in high power modes. This happens because of the asymmetry between Transmit and Receive modes, that is, while transmitting requires much more power than receiving, the total transmit time is, in general, negligible with respect to the time spent in receive mode. Transferring a single 512-bytes packet usually takes only a few milliseconds, whereas network interfaces usually stay in Receive mode, before transitioning into an Idle or Sleep mode, for an interval which may range from seconds to tens of seconds, depending on the specific network interface's hardware features. In fact, nodes tend to keep the radio in Receive mode for most of the time, to support several functions needed for improving the communication activity. For example, in order to always select the best (in terms of signal strength and quality) ad-hoc connection to the network during motion, nodes actively scan the available signals. In addition, in ad-hoc scenarios, neighbor discovery and ad-hoc routing are realized through the exchange of packets, which also requires the ability to monitor and receive information. This is also evident from Fig. 2(b), which shows the variation of per-node energy consumption with respect to the number of nodes considered. Although there are oscillations (due to random factors in the simulated mobility model), a general trend can be spotted, with Receive mode energy rising when the number of nodes, and consequently the overhead messaging, in-

Table 2
Simulation parameters.

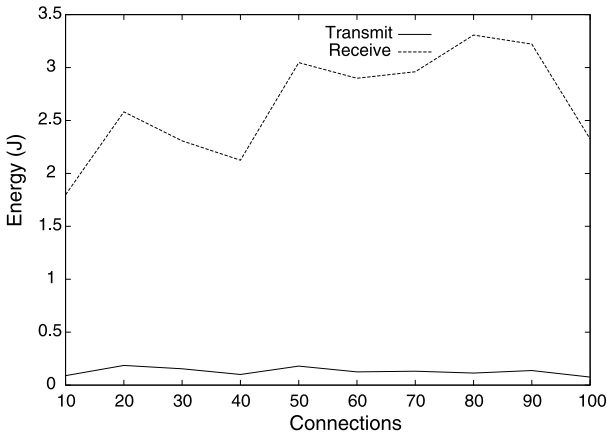
Generic parameters		
Simulated time (s)	*Single run*	500
Network environment	*Ad-hoc*	*DSDV routing*
Node interface and speed	*IEEE 802.11b*	11 Mb/sec
Mobility model	*Random waypoint*	1000×1000 m^2
Node pause time (s)	*Non stop moving*	0
Node speed (m/s)	*min* 0	*max* 20
Communication energy model parameters		
Idle power (W)	$P^{(i)}$	0.82
Sleep power (W)	$P^{(s)}$	0.046
Transition power (W)	P_t	0.2
Transmit power (W)	P_x	1.25
Receive power (W)	P_r	0.94
Output signal power (W)	P_o	0.031622777
Transition/wakeup time (s)	ξ_w, ρ_w	0.005
Per-bit transmit/receive time (s)	ξ_b, ρ_b	0.0000000909
Encryption energy model parameters		
1024-bits RSA key generation (mJ)	$\gamma(1024, RSA)$	270.13
1024-bits RSA sign (mJ)	$\sigma(1024, RSA)$	546.50
1024-bits RSA verify (mJ)	$\upsilon(1024, RSA)$	15.97
1024-bits DH key generation (mJ)	$\gamma(1024, DH)$	875.96
1024-bits DH key exchange (mJ)	$\chi(1024, DH)$	1046.50
128-bits AES key setup (μJ)	$\gamma(128, AES)$	7.83
256-bits AES key setup (μJ)	$\gamma(256, AES)$	9.92
128-bits AES encrypt/decrypt in ECB mode (μJ/B)	$\varepsilon(AES, 128, ECB)$	1.21
256-bits AES encrypt/decrypt in ECB mode (μJ/B)	$\varepsilon(AES, 256, ECB)$	1.64

creases. Such effect is definitely less evident for Transmit mode energy. A similar (but weaker) trend can be observed in Fig. 2(a) and in Fig. 2(c), where energy consumption is related, respectively, to the number of connections and the speed with which nodes travel across their environment. In such cases, the oscillations affect the results more heavily, because random values also determine factors such as the distance between the nodes that are establishing a connection. This phenomenon is clearly exacerbated as the speed of nodes increases, and consequently the continuous movement of nodes introduces an additional routing overhead, with significant random variations in Receive mode energy. It is worth noting that the transmission energy is almost independent of factors such as network density, traffic (number of connections) and node speed. No significant variation emerges in the charts in Fig. 2 for what concerns the transmission energy, whereas the receive energy exhibits a clear dependence on network density, besides being affected by the specific mobility patterns.

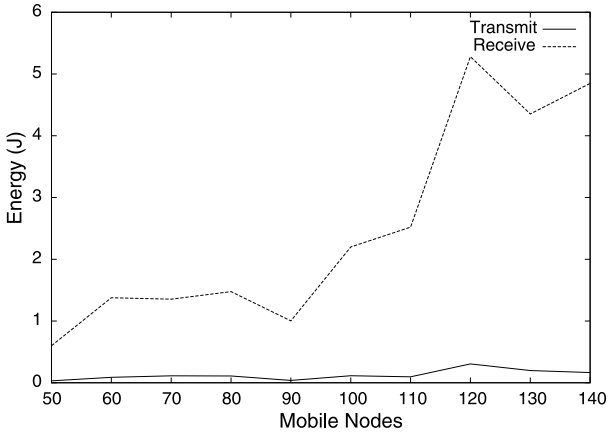
On the other hand, we can also pinpoint from Figs. 3(b) and 3(c) that both network density and speed do not have a significant impact on the average per-node energy drained by encryption activities. Indeed, it is the key size that affects the power consumption the most. Since the traffic model is the same in both the simulations with different key sizes, all the encryption energy plots exhibit the same variation, except for a scaling factor depending on the key size. This highlights the strong proportionality of the whole security energy with respect to the private-key encryption. By jointly observing the charts in Figs. 2 and 3, however, it can be appreciated that the amount of energy drained due to the communication and end-to-end security activities, while quite different in behavior, are almost comparable in their scale. Furthermore, it should be remarked that an increase in key sizes in the future, could raise the portion of energy required by cryptographic facilities. Therefore, optimization efforts should be devoted for both communication and security components, in order to achieve substantial improvements and sustainability.

6. Conclusions and future works

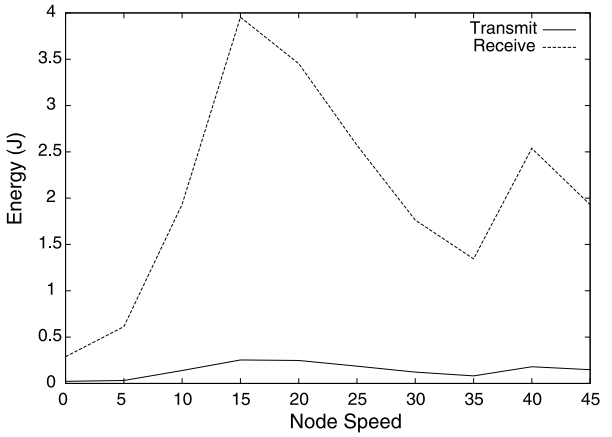
Due to the ever increasing necessity for multi-mode MTs to be always connected and able to reliably send/receive data, even in critical scenarios, the need for providing solutions that are able to cope with such situations, is getting stronger and stronger. However, hardware capacity restrictions and in particular battery constraints, require a careful analysis, mainly in order to optimize the use of available resources and consequently to extend the lifetime of involved MTs, primarily when they perform massive or frequent data communications. By carefully exploiting the proposed energy model, we may create the objective function for a global power optimization problem, which has the main aim of achieving secure communications, in a dynamic network scenario where a set of moving MTs need to maximize their operating life. Obviously, the individual model parameters may be used at the connection-setup time, in order to select the most energy-efficient solution among the available connection technologies, along with the best tradeoff between communication security and power consumption. This approach, leads to a novel energy-aware mobile communication service, allowing secure and reliable communication of significant amounts of data, by consuming the minimum energy budget possible. The proposed energy



(a) Transmit and receive energy with varying end-to-end connections. $MTs = 100, maxspeed = 20m/s$.

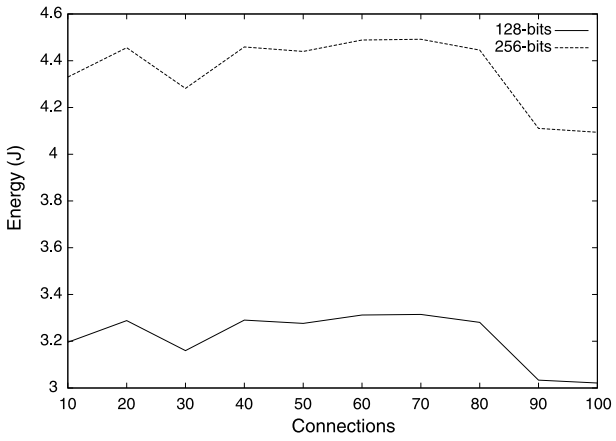


(b) Transmit and receive energy with varying network density. $Connections = 50, maxspeed = 20m/s$.

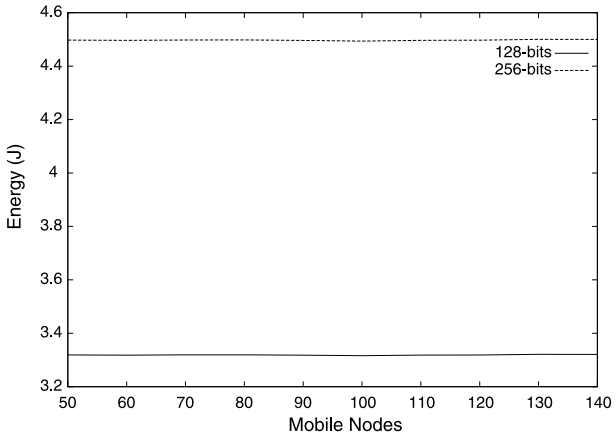


(c) Transmit and receive energy with varying node speed. $Connections = 50$, $MTs = 50$.

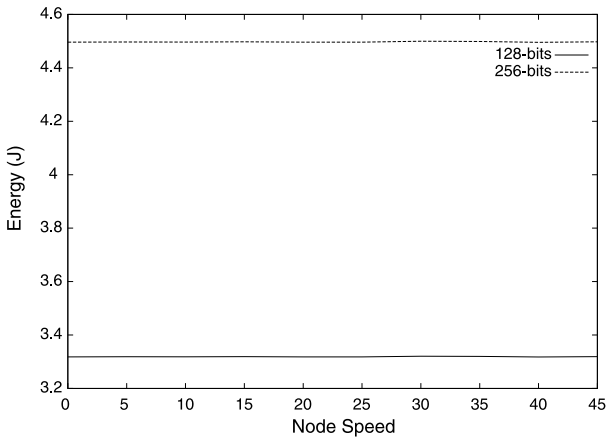
Fig. 2. Communication energy demand in high power modes.



(a) Encryption energy with varying end-to-end connections. $MTs = 100$, $maxspeed = 20m/s$.



(b) Encryption energy with varying network density. $Connections = 50$, $maxspeed = 20m/s$.



(c) Encryption energy with varying node speed. $Connections = 50$, $MTs = 50$.

Fig. 3. Security energy demand with different key sizes.

model may be used by MTs to choose, in a dynamic and adaptive manner, which are the "optimal" parameters, based on their own characteristics and on those of the underlying network, in order to maximize their lifetime. Finally, it is important to point out that particular attention should be paid during the selection of cryptographic algorithms to be used. Ideally, only those algorithms which are cryptographically strong, should be taken into account and evaluated from the energy consumption perspective.

References

[1] L.M. Feeney, M. Nilsson, Investigating the energy consumption of a wireless network interface in an ad hoc networking environment, in: Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 3, INFOCOM 2001, IEEE, 2001, pp. 1548–1557.
[2] L.M. Feeney, An energy consumption model for performance analysis of routing protocols for mobile ad hoc networks, Mob. Netw. Appl. 6 (3) (2001) 239–249.
[3] R.C. Shah, S. Roy, S. Jain, W. Brunette, Data mules: modeling and analysis of a three-tier architecture for sparse sensor networks, Ad Hoc Netw. 1 (2) (2003) 215–233.
[4] V. Shnayder, M. Hempstead, B.-r. Chen, G.W. Allen, M. Welsh, Simulating the power consumption of large-scale sensor network applications, in: 2nd International Conference on Embedded Networked Sensor Systems, ACM, 2004, pp. 188–200.
[5] J. Li, P. Mohapatra, Analytical modeling and mitigation techniques for the energy hole problem in sensor networks, Pervasive Mob. Comput. 3 (3) (2007) 233–254.
[6] N. Balasubramanian, A. Balasubramanian, A. Venkataramani, Energy consumption in mobile phones: a measurement study and implications for network applications, in: 9th ACM SIGCOMM Conference on Internet Measurement, ACM, 2009, pp. 280–293.
[7] H. Singh, S. Saxena, S. Singh, Energy consumption of TCP in ad hoc networks, Wirel. Netw. 10 (5) (2004) 531–542.
[8] F. Qian, Z. Wang, A. Gerber, Z.M. Mao, S. Sen, O. Spatscheck, Characterizing radio resource allocation for 3G networks, in: 10th ACM SIGCOMM Conference on Internet Measurement, ACM, 2010, pp. 137–150.
[9] J. Huang, F. Qian, A. Gerber, Z.M. Mao, S. Sen, O. Spatscheck, A close examination of performance and power characteristics of 4G LTE networks, in: 10th International Conference on Mobile Systems, Applications and Services, ACM, 2012, pp. 225–238.
[10] A. Castiglione, A. De Santis, A. Castiglione, F. Palmieri, U. Fiore, An energy-aware framework for reliable and secure end-to-end ubiquitous data communications, in: 5th International Conference on Intelligent Networking and Collaborative Systems, INCoS, 2013, pp. 157–165.
[11] L. Benini, A. Bogliolo, S. Cavallucci, B. Riccó, Monitoring system activity for OS-directed dynamic power management, in: 1998 International Symposium on Low Power Electronics and Design, ACM, 1998, pp. 185–190.
[12] L. Benini, A. Bogliolo, G. De Micheli, A survey of design techniques for system-level dynamic power management, IEEE Trans. Very Large Scale Integr. (VLSI) Syst. 8 (3) (2000) 299–316.
[13] J.R. Lorch, A.J. Smith, Software strategies for portable computer energy management, IEEE Pers. Commun. 5 (3) (1998) 60–73.
[14] A. Vahdat, A. Lebeck, C.S. Ellis, Every joule is precious: the case for revisiting operating system design for energy efficiency, in: 9th Workshop on ACM SIGOPS European Workshop: Beyond the PC: New Challenges for the Operating System, ACM, 2000, pp. 31–36.
[15] Y.-H. Lu, L. Benini, G. De Micheli, Operating-system directed power reduction, in: 2000 International Symposium on Low Power Electronics and Design, ACM, 2000, pp. 37–42.
[16] C.-L. Su, A.M. Despain, Cache design trade-offs for power and performance optimization: a case study, in: 1995 International Symposium on Low Power Design, ACM, 1995, pp. 63–68.
[17] C.E. Jones, K.M. Sivalingam, P. Agrawal, J.C. Chen, A survey of energy efficient network protocols for wireless networks, Wirel. Netw. 7 (4) (2001) 343–358.
[18] E. Uysal-Biyikoglu, B. Prabhakar, A. El Gamal, Energy-efficient packet transmission over a wireless link, IEEE/ACM Trans. Netw. 10 (4) (2002) 487–499.
[19] A. Rahmati, L. Zhong, Context-for-wireless: context-sensitive energy-efficient wireless data transfer, in: 5th International Conference on Mobile Systems, Applications and Services, ACM, 2007, pp. 165–178.
[20] L. Wang, J. Manner, Energy consumption analysis of WLAN, 2G and 3G interfaces, in: 2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing, IEEE Computer Society, 2010, pp. 300–307.
[21] N.I. Sarkar, Impact of traffic arrival distributions on an 802.11 ad hoc network: modeling and performance study, IEEE J. Sel. Areas Telecommun. 2 (5) (2012) 9–16.
[22] T. Hardjono, L.R. Dondeti, Security in Wireless LANs and MANs, Artech House, 2005.
[23] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM 21 (2) (1978) 120–126.
[24] D.W. Kravitz, Digital signature algorithm, US Patent 5,231,668, Jul. 27, 1993.
[25] W. Diffie, M. Hellman, New directions in cryptography, IEEE Trans. Inf. Theory 22 (6) (1976) 644–654.
[26] D. Johnson, A. Menezes, S. Vanstone, The elliptic curve digital signature algorithm (ECDSA), Int. J. Inf. Secur. 1 (1) (2001) 36–63.
[27] L. Law, A. Menezes, M. Qu, J. Solinas, S. Vanstone, An efficient protocol for authenticated key agreement, Des. Codes Cryptogr. 28 (2) (2003) 119–134.
[28] J. Daemen, V. Rijmen, The design of Rijndael: AES-the advanced encryption standard, Springer, 2002.
[29] R. Anderson, E. Biham, L. Knudsen, H. Technion, Serpent: a flexible block cipher with maximum assurance, in: The First AES Candidate Conference, 1998, pp. 589–606.
[30] R.L. Rivest, M.J. Robshaw, R. Sidney, Y.L. Yin, The RC6 block cipher, in: First Advanced Encryption Standard (AES) Conference, Citeseer, 1998.
[31] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, T. Tokita, Camellia: a 128-bit block cipher suitable for multiple platforms design and analysis, in: Selected Areas in Cryptography, Springer, 2001, pp. 39–56.
[32] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, Twofish: A 128-bit block cipher, NIST AES Proposal 15.
[33] L.M. Feeney, Energy-efficient communication in ad hoc wireless networks, in: Mobile Ad Hoc Networking, 2004, pp. 301–327.
[34] D. Halperin, B. Greenstein, A. Sheth, D. Wetherall, Demystifying 802.11 n power consumption, in: 2010 International Conference on Power Aware Computing and Systems, USENIX Association, 2010, p. 1.
[35] B. Tavli, Protocol architectures for energy efficient real-time data communications in mobile ad hoc networks, Ph.D. thesis, University of Rochester, 2005.
[36] T. Camp, J. Boleng, V. Davies, A survey of mobility models for ad hoc network research, Wirel. Commun. Mob. Comput. 2 (5) (2002) 483–502.
[37] J. Song, L. Miller, Empirical analysis of the mobility factor for the random waypoint model, in: Proc. OPNETWORK, 2002, pp. 600–700.
[38] N.R. Potlapally, S. Ravi, A. Raghunathan, N.K. Jha, Analyzing the energy consumption of security protocols, in: Proceedings of the 2003 International Symposium on Low Power Electronics and Design, ACM, 2003, pp. 30–35.
[39] N.R. Potlapally, S. Ravi, A. Raghunathan, N.K. Jha, A study of the energy consumption characteristics of cryptographic algorithms and security protocols, IEEE Trans. Mob. Comput. 5 (2) (2006) 128–143.
[40] S. McCanne, S. Floyd, ns Network Simulator, http://www.isi.edu/nsnam/ns/.

[41] J.-C. Cano, P. Manzoni, A performance comparison of energy consumption for mobile ad hoc network routing protocols, in: 8th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems, IEEE, 2000, pp. 57–64.
[42] A.S. Wander, N. Gura, H. Eberle, V. Gupta, S.C. Shantz, Energy analysis of public-key cryptography for wireless sensor networks, in: Third IEEE International Conference on Pervasive Computing and Communications, PerCom 2005, IEEE, 2005, pp. 324–328.
[43] X. Zhang, H.M. Heys, C. Li, Energy efficiency of encryption schemes applied to wireless sensor networks, J. Secur. Commun. Netw. 5 (7) (2012) 789–808.