On Energy-Security Tradeoffs and Cooperation for Wireless Ad Hoc Networks

Cristina Comaniciu

Stevens Institute of Technologies, Castle Point on Hudson, Hoboken New Jersey 07030-5991, USA; e-mail: Cristina.Comaniciu@stevens.edu

Abstract

In this paper we discuss the inherent security-energy tradeoffs that exist in wireless ad hoc networks. We propose a closed form cost computation approximation formula to determine the energy cost of monitoring for an intrusion detection algorithm based on its computational complexity and data size. Based on energy and security costs, we formulate a game theoretic distributed monitoring algorithm that enforces cooperative behavior for individual nodes by means of reward functions. Various energy-security tradeoffs operating points for the network intrusion detection can be achieved by tuning the rewards parameter.

Keywords: energy security tradeoff, ad hoc networks, intrusion detection, game theory.

1 Introduction

Security and energy are key performance metrics in wireless ad hoc networks, which have been traditionally individually addressed in the research literature.

Journal of Cyber Security and Mobility, 53–64.

Security attacks on these networks can range from being cyber based, (e.g. denial of service attacks at the network layer) to physical attacks (e.g. jamming leading to a physical layer specific denial of service attack). Moreover, the security monitoring and attack response can also be managed at various layers of the protocol stack, by employing physical layer specific techniques (e.g. dynamic channel allocation, power control, interference cancellation), MAC (Medium Access Control) techniques, or network layer oriented techniques (such as intrusion detection monitoring). While security is an important key performance metric, many of the security monitoring and assurance techniques require extensive computations and data manipulations which may put a high toll on the energy resource, which is at a premium for wireless nodes. With security and energy in mind, we conjecture that in these wireless systems, computational and physical resources are tightly inter-related.

While sophisticated algorithms for security assurance have been developed in the literature (e.g. intrusion detection systems, encryption) the general consensus is that they are very computational intensive and thus they put a high toll on individual devices' battery life. There is an inherent trade-off with respect to the level of security that can be achieved and the amount of energy expenditure that it is required.

Our intrusion detection problem focuses on thwarting attacks that aim to maliciously utilize the systems' resources for illicit transmissions, or to implement energy depletion attacks (a form of denial of service attacks), by requesting excess forwarding of malicious empty packets (attacks at cyber level) or creating excessive interference to communicating devices (attacks at the physical layer).

To detect these kinds of attacks, monitoring should be deployed at the network level to detect anomalous behavior, and at the physical layer to detect illicit transmissions. Continuous monitoring will deplete the energy resources of individual nodes even in the absence of an energy depletion attack. There is an inherent energy-security tradeoff that influences the amount of monitoring that is optimal for individual devices.

As being a part of a bigger network, nodes can cooperate for better overall performance efficiency. In a relatively densely deployed network, multiple nodes will detect the same security event. It becomes apparent that not all nodes should be required to monitor and report, but reporting events from multiple nodes can be aggregated by a sink node to obtain a more accurate and

robust detection and localization of the intruder. The main goal for our security monitoring task is to accurately, timely and robustly detect and localize an intruder in the network, while optimizing the energy efficiency of the system.

Energy and security issues have been traditionally investigated as independent subjects in the wireless networks literature. There is a significantly rich literature on developing effective intrusion detection algorithms and hard to attack encryption/decryption protocols. Similarly, energy efficiency for limited battery devices has been extensively studied especially in the context of wireless sensor networks.

There is very little work however, in understanding the cross-coupling between these two key metrics [1, 2–4, 5, 6–8] for wireless networks. In recent years, there has been an increased interest on developing more energy efficient security methods [9–15], as well as on exploiting cooperation for more efficient monitoring in networks [16–19]. More recently, an increased interest has risen on quantifying the energy/power tradeoffs for various encryption algorithms [6–8], but to the best of our knowledge no work has addressed this issue in the context of cooperation across nodes in a network, except for our preliminary work in [1].

In this paper we analyze the problem of cooperative intrusion detection for wireless ad hoc networks, and we propose a game theoretic framework to determine equilibrium monitoring strategies for individual nodes, and to analyze the achievable energy-security tradeoffs in the network. We address two different security breaches scenarios which require intrusion detection monitoring at the physical layer and at network layer, respectively.

2 The Security Problem

We consider a wireless ad hoc network in which IDSs (intrusion detection systems) are deployed at individual nodes to detect malicious behavior in the network. One of the scenarios considers the task of illicit wireless transmission detection in an ad hoc network in which nodes may behave selfishly. The other scenario considers denial of service attacks (DoS) which require monitoring at the network level. For the first scenario, monitoring implies continuous spectrum sensing to determine the presence of illicit transmissions, while for the later scenario, each individual node needs to collect and analyze large amounts of data to determine anomalous behavior.

We note that for each scenario, continuous monitoring at individual nodes may put a high toll on system resources, and as such, for a more energy efficient network design, the monitoring burden can be shared among the nodes participating in the network. A distributed solution to organize the nodes to cooperate for IDS monitoring is highly desirable to reduce the overhead generally associated with centralized solutions. In this work, we propose such a distributed solution based on a game theoretic formulation. Each node decides to monitor or not independently, aiming to maximize a utility function which represents a balance between the gains obtained by monitoring and the energy costs involved. Since the results of the monitoring are shared with the entire neighborhood, an important issue of selfishness arises, yielding a problem similar with the classic tragedy of the commons scenario.

3 A Game Theoretic Solution for Cooperation

A game theoretic formulation can be proposed to analyse the energy-security tradeoffs for the intrusion detection monitoring problem. These tradeoffs can be captured by appropriately defining a utility function that incorporates the cost of monitoring and the security gains. A simple finite strategic form game can illustrate the tradeoffs involved and can be used to design a distributed monitoring algorithm for the network that achieves a prescribed security-energy tradeoff.

The intrusion detection game can be set-up as an adversarial game, in which the players are the nodes in the network defending the network security against a potential malicious node in the system. The players' actions can be defined as {monitor, not monitor} for the defending nodes, and {attack, not attack}, for the malicious node.

For illustration purposes we assume that users know that an attacker is present in the system, and thus the game becomes a complete information game, which can be modelled as a finite strategic game. We note that more complex scenarios with incomplete information can be analysed as presented in our previous work in [1], but for illustrating the energy-security tradeoffs involved in the intrusion detection monitoring problem, and for analyzing the effect of nodes' cooperation, the simplest case will suffice.

We assume that users decide to monitor or not, based on their desired security level expressed as a security gain ($s > 0$), their current cost of monitoring ($m > 0$), and their defined utility function for each option. Assuming the

Table 1 An example security monitoring game model.

		Player j	
		Monitor	Not Monitor
Player i	Monitor	$(s-m, s-m)$	$(s-m, s)$
	Not Monitor	$(s, s-m)$	(0.0)

malicious node is present in the system and has only one strategy: attack, two defending players i, j, can play against each other as illustrated in Table 1. If one of the players monitors, both players gain in security, while if none of them monitors they get zero utility by losing the security value.

For the above game, under the assumption that $s > m$, we have two Nash equilibria (monitor, not monitor) and (not monitor/monitor) characterized by the utilities $(s, s-m)$ and $(s-m, s)$. We can see that we do not know which equilibrium will be played in practice. There is also a mixed strategy equilibrium, determined based on the indifference principle [20], such that the players are indifferent between their actions and consequently randomize their choice of action.

To impose a certain outcome for the game, we introduce rewards for monitoring, r_i, and we impose that players play a mixed strategy equilibrium, i.e., each player will monitor with a probability p.

Expanding the game to M potential defender players that see similar events, the equilibrium for the game can be derived as follows.

Let p be the probability of contributing to the monitoring for an arbitrary defending node. The probability of no contribution by a node is $(1-p)$. The expected payoff that player (node) i will receive by monitoring is

$$u_i(monitor) = s_i - m_i + r_i. \tag{1}$$

The expected payoff that player $i$will receive if it does not monitor can be determined as:

$$u_i(not\_monitor) = s_i(1-(1-p)^{M-1}), \tag{2}$$

which is computed by observing that a $s_i$security value is gained if at least one node is contributing, and a zero utility is achieved if nobody monitors.

Using the indifference principle [20], we can find the equilibrium strategy, i.e., the equilibrium probability that a node will monitor will be given as:

$$p_i^* = 1 - \sqrt[M-1]{\frac{m_i - r_i}{s_i}}. \tag{3}$$

To achieve fairness across nodes, the rewards can be chosen such that all users monitor with the same probability, and thus use the same amount of resources for monitoring purposes.

The probability of monitoring influences the overall detection probability, which can be computed as the probability that at least one node is contributing to the monitoring activities in the cluster.

$$P_D = (1 - (1 - p^*)^M). \tag{4}$$

As a final observation, we note that a mathematical value for the security gain is usually hard to determine in practice, and as such, a practical approach would be to express the equilibrium probability as a function of the monitoring versus security cost ratio (which characterizes the relative importance the application has on energy or security), as well as a function of reward versus security gain ratio, which can be treated as a parameter and adjusted accordingly for a desired performance.

4 Energy Monitoring Cost

The two intrusion detection scenarios described in the previous section can be treated similarly, except that for the first one, the monitoring is done by spectrum sensing at the physical layer, while for the latter network data needs to be collected and analyzed using a computationally intensive algorithm. With this respect, the two monitoring game formulations differ solely by the computation of the monitoring cost.

In our paper in [23], we have shown that the monitoring cost for the physical layer spectrum sensing monitoring can be readily determined based on the specifications of the receiver.

For the latter scenario, our goal is to determine a generic formula for the energy consumption associated with a computational algorithm running on embedded systems (e.g., intrusion detection monitoring algorithms — IDS) based on the complexity and type of instructions involved in the algorithm's implementation.

In our previous work in [1], we have proposed a first order approximation model for energy consumption estimation for a C based implementation code on a typical wireless ad hoc network microcontroller (Freescale Semiconductor's MC9S08GT60). Our model is based on the observation in [21] that, to a first order approximation, the current consumption of a piece of code

is independent of the code, and depends only on the operating voltage and frequency of the processor. The first order software energy estimation model is then simply

$$E_{tot} = V_{dd} I_0(V_{dd}, f)\Delta t, \tag{5}$$

where, E_{tot} is the total energy consumed in executing the program, V_{dd} is the supply voltage, Δt is the program execution time, and $I_0(V_{dd}, f)$ is the supply current at the given V_{dd} level and the given operating frequency f.

We have verified that this equation holds for a general class of microcontrollers used in wireless ad-hoc sensor networks, by extensive experimentation using Freescale Semiconductor's MC9S08GT60 Microcontroller.

These results naturally lead to the energy consumption metric being determined mainly as a function of the execution time Δt of the programs, given V_{dd} and I_0 (V_{dd}, f) in (5).

The execution time Δt *of* a specific program is directly related to the time complexity of the associated algorithm. The time complexity function ***t(n)*** of an algorithm takes the problem size (instance characteristic) ***n*** as the argument and returns the number of program steps as the result. A program step is loosely defined as a syntactically or semantically meaningful segment of a program that has an execution time that is independent of the instance characteristics counts (a step could be an addition, a multiplication, a comparison, etc.). The instance characteristic ***n*** is the parameter characterizing the size of the problem such as the "***n-element*** **array** being sorted".

Using the time complexity function, we can use the following equation for finding the execution time Δt *of* a program written in a high level language (e.g. C programming language):

$$\Delta t = \frac{t(n)Nc}{f}, \tag{6}$$

where $t(n)$ is the time complexity function giving the total number of steps, n is the instance characteristic, N is the average number of machine instructions per step count, c is the average number of machine cycles per machine language instruction and f is the operation frequency of the computing platform.

From (5) and (6), a complete first order energy equation can be written as:

$$E_{\text{tot}} = V_{DD} I_0(V_{DD}, f)\frac{t(n)Nc}{f} \tag{7}$$

Since this formula uses an average value for N, it only gives a first approximation of the energy consumption. However, to get a more precise estimation, the value of $t(n)$ can be modified to account for the different number of instructions a statement is using on the targeted CPU.

Equation (7) will allow us to predict the energy consumption of a program for different problem sizes, as a function of the complexity of the algorithm. It can be used to determine the energy cost metric for an IDS monitoring implemented in C on a microcontroller in sensor networks.

In our previous work in [1], we have determined the energy consumption for a particular cross-feature IDS monitoring for Denial-of Service Attacks. To determine the impact of the IDS on the battery life of a wireless node, we used the "Battery Life Estimation Model" [22] of a ZigBee Wireless ad-hoc network node using the same microcontroller (MC9S08GT60) and Freescale Semiconductor's MC13192 RF transceiver. Our comparison findings illustrate that a ZigBee node consumes roughly three times more energy when running an IDS algorithm.

5 Energy-Security Tradeoffs

We illustrate with a simple example the energy-security tradeoffs that can be achieved in a wireless network with 10 trusted nodes that participate in the monitoring game. In Figure 1 we show how the security level (probability of detection) for the cluster changes based on the selection of the

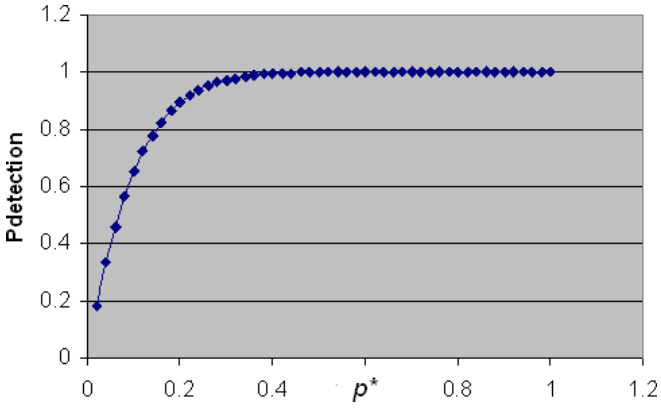


Figure 1 Detection probability as a function of nodes' monitoring probability.

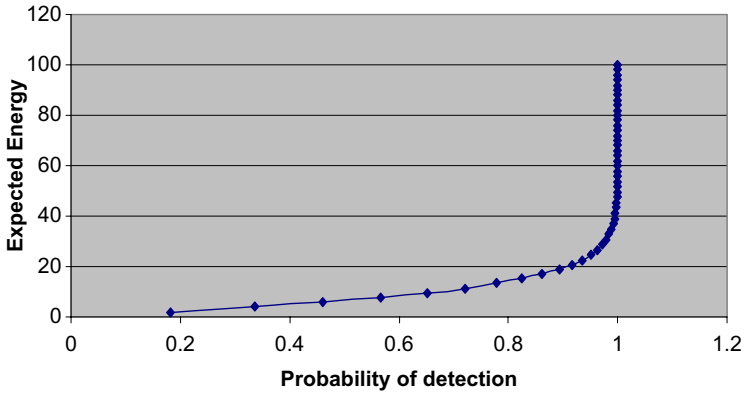


Figure 2 Energy-security tradeoffs for intrusion detection monitoring.

monitoring probability p^*. As we have mentioned earlier, specific p^* values can be imposed by selecting appropriate rewards for each node. The probability of detection is then calculated for different values of p^* by using Equation (3). It can be seen that high security levels (between 0.89 and 0.99) can be achieved for low monitoring probabilities (between 0.2 and 0.4).

In Figure 2 we illustrate how the expected total energy consumption of the cluster changes with the change of the prescribed security level for the cluster. For these results we assume that the energy spent by the IDS for each of the IDS nodes is 10 unit of battery capacity in the selected unit time frame (time slot). Expected total energy of the cluster for each time slot can be calculated as:

$$E = \sum_{k=1}^{10} P(\#\text{ monitoring} = k)k\varepsilon,$$

where up to k nodes may contribute to the monitoring, each spending ε units of energy.

It can be seen from the Figure 2 that as the required probability of detection value gets closer to 1 the expected total energy consumption increases rapidly.

6 Conclusions

In this paper we have illustrated the energy-security tradeoffs that are inherently associated with any security monitoring problem, using some simple classic examples of intrusion detection in wireless ad hoc networks.

Our presented analysis was based on a game theoretic formulation that allows for the design of a distributed monitoring algorithm which achieves a prescribed security level for the network while preserving the energy resources of individual nodes. The proposed reward function played a dual role of incentivizing cooperation, as well as serving as a tuning parameter to adjust the network operation point for a desired energy-security tradeoff.

Acknowledgements

The author would like to thank Seyhun Mehmet Futaci for obtaining some of the analytical and experimental results presented in this paper as part of his thesis work.

References

[1] S. Mehmet Futaci, K. Jaffres Runser, and C. Comaniciu. On modeling energy-security trade-offs for distributed monitoring in wireless ad hoc networks, MILCOM, November 2008, pp. 1–7.

[2] Y. Li, H. Man, and C. Comaniciu. A game theoretic approach to efficient mixed strategies for intrusion detection. *Proceedings of IEEE International Conference on Communications (ICC 2006)*.

[3] Y. Liu, C. Comaniciu, and H. Man. Modeling misbehavior in ad hoc networks: A game theoretic approach for intrusion detection. *International Journal of Security and Networks (IJSN)*, 2006.

[4] Y. Liu, C. Comaniciu, and H. Man. A bayesian game approach for intrusion detection in wireless ad hoc networks. In *Proceedings of GameNets (Workshop on Game Theory for Networks)*, October 2006, Pisa, Italy.

[5] H. Otrok, N. Mohammed, L. Wang, M. Debbabi, and P. Bhattacharya. A moderate to robust game theoretical model for intrusion detection in MANETs, *International Conference on Wireless and Mobile Computing, Networking and Communications (WIMOB)*, October 2008, pp. 608–612.

[6] A. Hodjat and I. Andverbauwhede. The energy cost of secrets in ad-hoc networks. *IEEE Circuits and Systems Workshop on Wireless Communications and Networking*, 2002.

[7] N. Potlapally, N. Ravi, S. Raghunathan, and N. Jha. Analyzing the energy consumption of security protocols. *International Symposium on Low Power Electronics and Design*, 30–35, 2003.

[8] R. Chandramouli, S. Bapatla, K.P. Subbalakshmi, and R.N. Uma. Battery power-aware encryption. *ACM Trans. on Information and Systems Security (TISSEC)*, 2006.

[9] C. Chich-Chun, S. Muftic, and D.J. Nagel. Measurement of energy costs of security in wireless sensor nodes. *IEEE 18th International Conference on Computer Communications and Networks*, August 2007, pp. 95–102.

[10] Y. Bidi, C. Huifang, Z. Wendao, and Q. Peiliang. An energy-aware random pairwise keys scheme in wireless sensor networks. *IEEE Sixth World Congress on Intelligent Control and Automation (WCICA)*, 2006, pp. 114–118.

[11] B.-C.C. Lai, D.D. Hwang, S.P. Kim, and I. Verbauwhede. Reducing radio energy consumption of key management protocols for wireless sensor networks. *IEEE International Symposium on Low Power Electronics and Design*, ISLPED, August 2004, pp. 351–356.

[12] P. Trakadas, T. Zahariadis, H.C. Leligou, S. Voliotis, and K. Papadopoulos. Analyzing energy and time overhead of security mechanisms in wireless sensor networks. *IEEE International Conference on Systems, Signals and Image Processing (IWSSIP)*, June 2008, pp. 137–140.

[13] Y. Lei and L. Jianzhong. SpyMon: Hidden network monitoring for security in wireless sensor networks. *IEEE International Conference Mobile Ad Hoc and Sensor Systems (MASS)*, October 2008, pp. 328–333.

[14] D. Jain and V.M. Vokkrane. Energy-efficient target monitoring in wireless sensor networks. *IEEE Conference on Technologies for Homeland Security*, 2008.

[15] R. Chandramouli, S. Bapatla, K.P. Subbalakshmi, and R.N. Uma. Battery power-aware encryption. *ACM Trans. on Information and Systems Security (TISSEC)*, 2006.

[16] P. Inverardi, L. Mostarda, and A. Navarra. Distributed IDSs for enhancing security in mobile wireless sensor networks. *IEEE International Conference on Advanced Information Networking and Applications*, April 2006, pp. 116–120.

[17] P. Techateerawat and A. Jennings. Energy efficiency of intrusion detection systems in wireless sensor networks. *IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology Workshops*, December 2006, pp. 227–230.

[18] Y. Huang and W. Lee. A cooperative intrusion detection system for ad hoc networks. In *Proceeding of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 135–147, October 2003.

[19] O. Kachirski and R. Guha. Intrusion detection using mobile agents in wireless ad hoc networks. In *Proceedings of the IEEE Workshop on Knowledge Media Networking*, pp. 153–158, July 2002.

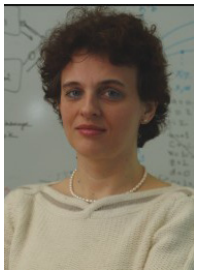
[20] D. Fudenberg and D. Levine. *The Theory of Learning in Games*. MIT Press, 1998.

[21] A. Sinha and P.A. Chandrakasan. JouleTrack — a web based tool for software energy profiling. *ACM Design Automation Conference*, June 2001.

[22] Seminar notes. ZigBee technical training seminar. *Freescale Semiconductor and EBV Electronics*, Istanbul, Turkey, February 2005.

[23] Q. Shi and C. Comaniciu. Efficient cooperative detection in wireless sentinel networks. In *Proceedings of CISS*, March 2010, Princeton, NJ.

Biography



Cristina Comaniciu received the M.S. degree in Electronics and Telecommunications from the Polytechnic University of Bucharest in 1993, and the Ph.D. degree in Electrical and Computer Engineering from Rutgers University in 2002. From 2002 to 2003 she was a postdoctoral fellow with the Electrical Engineering Department at Princeton University. Since 2003, she is with Stevens Institute of Technology, where she is currently an Associate Professor and Graduate Program Director. She served as an Associate Editor for IEEE Communication letters from 2006–2011.

Cristina is a co-recipient of the 2007 IEEE Marconi Best Paper Prize Award in Wireless Communications, and co-author of the book "Multiuser Detection in Cross-Layer Design", Springer 2005. Cristina was also recently awarded the Rutgers School of Engineering Medal of Excellence Award for the Distinguished Young Alumnus.

Her research interests include cooperative protocols for spectrum sharing and interference mitigation, cross-layer design, game theoretic approaches for energy aware wireless networks, radio resource management for cellular and ad hoc networks and security tradeoffs for wireless networks.