Effect of Intrusion Detection on Reliability of Mission-Oriented Mobile Group Systems in Mobile Ad Hoc Networks

Jin-Hee Cho, *Member, IEEE*, Ing-Ray Chen, *Member, IEEE*, and Phu-Gui Feng

***Abstract*—For mission-oriented mobile group systems designed to continue mission execution in hostile environments in the presence of security attacks, it is critical to properly deploy intrusion detection techniques to cope with insider attacks to enhance the system reliability. In this paper, we analyze the effect of intrusion detection system (IDS) techniques on the reliability of a mission-oriented group communication system consisting of mobile groups set out for mission execution in mobile ad hoc networks. Unlike the common belief that IDS should be executed as often as possible to cope with insider attacks to prolong the system lifetime, we discover that IDS should be executed at an optimal rate to maximize the mean time to failure of the system. Further, the optimal rate at which IDS is executed depends on the operational conditions, system failure definitions, attacker behaviors, and IDS techniques used. We develop mathematical models based on Stochastic Petri nets to identify the optimal rate for IDS execution to maximize the mean time to failure of the system, when given a set of parameter values characterizing the operational conditions, and attacker behaviors.**

***Index Terms*—Intrusion detection, intrusion detection system, mean time to security failure, mission-oriented group communication systems, mobile ad hoc networks.**

ACRONYMS

IDS	Intrusion Detection System
MANET	Mobile Ad_Hoc Network
GCS	Group Communication System
MTTSF	Mean Time To Security Failure
GDH	Group Diffie_Hellman
VS	View Synchrony
SF	Security Failure
SPN	Stochastic Petri net

NOTATION

λ	Arrival rate of join requests (times/sec)
μ	Arrival rate of leave requests (times/sec)
T_{IDS}	Base intrusion detection interval used in the intrusion detection function
λ_c	Base node compromising rate used in the attacker function
λ_q	Group data communication rate per node (times/sec)
$p1$	False negative probability of host_based IDS
$p2$	False positive probability of host_based IDS
P_{fn}	False negative probability of voting_based IDS
P_{fp}	False positive probability of voting_based IDS
b_{GDH}	Length of an intermediate value in applying GDH.3 (bits)
r	Radius of the operational area (meters)
R	Wireless per_hop radio range (meters)
σ	Mobility rate per node
BW	Wireless network bandwidth (Mbps)
N_{init}	Number of trusted member nodes in the system initially
N	Number of active member nodes in a group
$N_{majority}$	Majority number of members out of m vote_participants (i.e., $\geq \lceil m/2 \rceil$)
N_{good}	Number of trusted members in a group
N_{bad}	Number of untrusted members in a group
m_d	Degree of nodes that have been detected as compromised by IDS
m_c	Degree of compromised nodes currently in a group
δ	Detection function that returns a periodic detection rate based on m_d
θ	Attacker function that returns time taken to compromise a node based on m_c
p	A base or exponent used in δ, and θ
m	Number of vote_participants in voting_based IDS against a target node
T_{cm}	Communication time for broadcasting a rekeying message (sec)
$\mu_{nm,i}$	Group partitioning rate when the number of groups in the system is i
$\lambda_{np,i}$	Group merging rate when the number of groups in the system is i
S_i	System sojourn time in state i (i.e., when i groups are present in the system)

Manuscript received August 31, 2008; revised April 15, 2009; accepted July 22, 2009. First published February 08, 2010; current version published March 03, 2010. Associate Editor S. Shieh.

J.-H. Cho is with the Army Research Laboratory, Adelphi, MD 20783-1197 USA (e-mail: jinhee.cho@arl.army.mil).

I.-R. Chen is with the Department of Computer Science, Virginia Tech, Blacksburg, VA 24061 USA (e-mail: irchen@vt.edu).

P.-G. Feng is with The MITRE Corporation, Bedford, MA 01730-1420 USA (e-mail: pfeng@mitre.org).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TR.2010.2040534

$E[Y(\infty)]$	Expected accumulated reward until absorption
$P_i(t)$	Probability of state i at time t
r_i	Reward assignment at state i

I. Introduction

MANY mobile applications in wireless networks such as military battlefield, emergency response, online gaming, and collaborative work are based on the notion of mobile groups. For military applications, the group communication system (GCS) designed for mission execution often consists of *mission-oriented* mobile groups set out for mission execution. The mission is to be completed despite the presence of malicious attackers with intent to break security, and cause the system to fail; as well as user mobility, which may cause mobile groups to be partitioned, and later merged again when network connectivity is resumed. We are interested in knowing design conditions for employing intrusion detection system (IDS) techniques that can enhance the reliability, and thus prolong the lifetime, of such a mission-oriented GCS. Here, by "lifetime," we mean the failure time of the GCS.

Designing security protocols for mobile groups in mobile ad hoc networks (MANETs) faces many technical challenges due to unique characteristics of MANETs including resource-constrained environments in bandwidth, memory size, battery life and computational power, openness to eavesdropping and security threats, unreliable communication, no infrastructure support, and rapid changes in topology due to node mobility which often cause mobile group merge/partition events to occur dynamically. Three types of actions may be taken against malicious attacks: prevention, detection, and recovery. Prevention techniques (e.g., encryption or authentication) can be employed to reduce intrusion. However, security holes [30] cannot be perfectly eliminated. Thus, IDS protocols have been introduced as a second line of defense, and have become essential for systems such as mission-oriented GCSs with the goal of high-survivability and availability to prolong the system lifetime [30]. In this work, we are interested in the effect of IDS on the reliability, and the system lifetime of a GCS consisting of mission-oriented mobile groups in MANETs. In particular, we like to identify optimal design settings for executing IDS to prolong the system lifetime of mission-oriented GCSs.

Approaches to extend the system or network lifetime in wireless networks, mostly in wireless sensor networks [3], [5], [7], [13], [16], [20], [27], [31], and MANETs [11], [24], [25], have generally been considered in terms of reducing energy consumption. Many energy-efficient algorithms have been devised to prolong network lifetime while meeting performance requirements with minimum energy consumption. A system failure is often defined as when the first node fails [5], [7], [11], [13], [16], [20], [23], [24], [27], [31], or when a majority of nodes (say more than one half) fail due to energy depletion [3]. To the best of our knowledge, no prior work has been done considering the effect of security threats versus counter IDS techniques on security-induced system failure time in wireless networks where security is a prime concern. Further, in the case of mission-oriented GCSs deployed in high hostile environments, no previous work has been done in identifying optimal design settings to prolong the system lifetime to improve the mission success probability. Our work reported in this paper is the first to address this issue.

Our work has its root in model-based quantitative analysis [17]. In the literature, we have seen growing interests in applying model-based quantitative analysis to security analysis recently. Zhang *et al.* [29] analyzed several group rekeying algorithms in wireless environments, and evaluated their performance characteristics. No intrusion was considered, however. Dacier *et al.* [4] proposed a novel approach to model the system as a privilege graph demonstrating operational security vulnerabilities, and transformed the privilege graph into a Markov chain based on all possible successful attack scenarios. Jonsson *et al.* [8] presented a quantitative Markov model of attacker behaviors using data obtained from several experiments conducted over two years. They postulated that the process describing an attacker may be divided into multiple phases, such as learning, standard attack, and innovative attack. Popstojanova *et al.* [21] presented a state transition model to describe dynamic behaviors of intrusion tolerance systems. Their model includes a framework to define the vulnerability, and the threat set. Madan *et al.* [14], [15] employed a Semi-Markov Process (SMP) model to evaluate security attributes of an intrusion-tolerant system known as the SITAR system. Based on particular attack scenarios, they associated system states with the failure of security goals such as availability, data integrity, and data confidentiality. A steady-state analysis has been used to obtain dependability measures such as availability. A transient analysis with absorbing states has been used to obtain security measures such as *mean time to security failure* (*MTTSF*), similar to the computation of the *mean time to failure* (*MTTF*) in reliability analysis. Stevens *et al.* [26] also proposed a networked intrusion tolerant information system using a model-based validation technique based on probabilistic modeling. Their model-based results were employed, not only to guide the system's design, but also to determine whether or not a given survivability requirement was met. Wang *et al.* [28] utilized a higher-level formalism for security analysis of intrusion tolerant systems. Patcha *et al.* [18] proposed a game theoretic formulation for intrusion detection in MANETs. Li *et al.* [10] utilized behavior knowledge for evaluation of intrusion detection systems.

Like prior work, we also use *MTTSF* as a measure to reflect the expected system lifetime, representing a measure against *loss of service availability*, or *system integrity*. We show that there exist optimal design settings for deploying IDS techniques such that the security-induced failure time (or *lifetime* for short) is maximized. Specifically, we identify the optimal rate at which IDS should be executed to maximize the system lifetime, when given a system failure definition explicitly defining how the system is considered as having failed, and a set of parameter values characterizing the operational conditions and attacker behaviors.

The main contributions of this paper are as follows. First, we consider the effect of security threats, and counter IDS techniques on system lifetime of a mission-oriented GCS consisting of mobile groups in MANETs. Second, we develop

mathematical models to identify the optimal intrusion detection rate at which *MTTSF* is maximized through analyzing the tradeoff between positive effects of IDS versus negative effects of IDS (generating false positives/negatives by triggering IDS), using voting-based IDS as an example. Lastly, we show that the analysis methodology developed is generally applicable to varying network conditions (nodes being able to communicate with each other through single-hop or multi-hop), and varying system failure definitions for calculating *MTTSF* of a GCS consisting of mission-oriented mobile groups in MANET environments.

II. System Model

This paper concerns the failure time of a mission-oriented GCS consisting of mobile groups in MANETs equipped with intrusion detection to deal with inside attackers. The notion of a mobile group is defined based on "connectivity." When all nodes are connected, there is only a single group in the system. That is, group members must maintain connectivity to be in the same group. The GCS, and its constituent mobile groups are "mission-oriented" in the sense that a mobile group may be partitioned into several groups due to network partition derived from node mobility, or node failure.

However, these partitioned groups will still continue with the same mission assigned throughout their lifetime. Later, when two or more partitioned groups merge into one, the merged group will still continue with the same mission execution. Therefore, mission execution is an application-level goal built on top of connectivity-oriented group communications.

Each mobile group performs secure group communications by using a symmetric key, called the *group key*, shared by group members. The group key is employed to encrypt the message sent by a member to others in the group for *confidentiality*. The group key is rekeyed upon group member join/leave/eviction, and group partition/merge events to preserve secrecy [19]. We assume that a contributory key agreement protocol, such as Group Diffie-Hellman (GDH), is used for group key rekeying for decentralized control, and to eliminate a single point of failure. *Service availability* is achieved by maximizing system lifetime. We use *MTTSF* as an indicator for performance optimization. In particular, we shall identify optimal intrusion detection intervals to maximize *MTTSF*, leading to improved service availability.

We assume that each member has a private key, and its certified public key, available for *authentication* purposes. The mission-oriented mobile group system is bootstrapped with the public keys of all group members preloaded into every node. There is no certificate authority (CA) in the MANET during the mission period, and the public key of a node is assumed not to be revoked during the mission time. When a new member joins a group, the new member's identity is authenticated based on the member's public/private key pair by applying the challenge/response mechanism. A node's public key therefore serves as the *identifier* of the node, and we will use this term in our paper.

The workload and operational conditions of a mission-oriented GCS in MANETs can be characterized by a set of parameters. In particular, we assume that a node may leave a group voluntarily with rate μ, and may rejoin any group with rate λ due to tactical reasons. Then, the probability that a node is in any group is $\lambda/(\lambda+\mu)$, and the probability that it is not in any group is $\mu/(\lambda+\mu)$. Nodes can move freely with a mobility rate of σ. Reliable transmission is a system requirement for secure group communications. We assume that *view synchrony (VS)* is guaranteed in GCSs [25], which guarantees that messages are delivered reliably, and in proper order under the same membership view. That is, a receiver will see the same membership view as viewed by the sender.

Two types of IDS protocols are being considered in this paper as applicable to mission-oriented GCSs in MANETs: *host-based IDS,* and *voting-based IDS*.

In host-based IDS, each node performs local detection to determine if a neighboring node has been compromised. The effectiveness of IDS techniques applied (e.g., misuse detection or anomaly detection) for host-based IDS is measured by two parameters: the false negative probability $(p1)$, and false positive probability $(p2)$. Host-based IDS is preinstalled in each host.

The second type is voting-based IDS for cooperative detection based on majority voting. Voting-based IDS derives from the fault tolerance concept based on majority voting for evicting a target node in the context of sensor networks [2]. Each node is preinstalled with host-based IDS to collect information to detect the status of neighboring nodes. Periodically, a target node would be evaluated by m vote-participants dynamically selected, where m is a design parameter. If the majority of m nodes decided to vote against the target node, then the target node would be evicted from the system. Bad nodes in the system can collude by (a) evicting good nodes by always voting "no" to good nodes, and (b) keeping bad nodes in the system by always voting "yes" to bad nodes. Our voting-based IDS protocol adds intrusion tolerance to tolerate collusion of compromised nodes in MANETs as it takes a majority of bad nodes among m nodes to work against the system. We characterize voting-based IDS by two parameters: false negative probability (P_{fn}), and false positive probability (P_{fp}). These two parameters may be calculated based on (a) the *per-node* false negative, and positive probabilities ($p1$, and $p2$) of host-based IDS in each node; (b) the number of vote-participants, m, selected to vote for or against a target node; and (c) an estimate of the current number of compromised nodes which may collude with the objective to disrupt the service of the system. Because m nodes are selected to vote, if the majority of m voting-participants casts negative votes against a target node, the target node is considered compromised, and will be evicted from the system.

For the selection of m vote-participants in voting-based IDS, each node periodically exchanges its routing information, location, and *identifier* with its neighboring nodes. With respect to a target node, all neighbor nodes that are within a number of hops from the target node are candidates as vote-participants. A coordinator is selected randomly so that the adversaries will not have specific targets. We add randomness to the coordinator selection process by introducing a hashing function that takes in the *identifier* of a node concatenated with the current location of the node as the hash key. The node with the smallest returned hash value would then become the coordinator. Because candidate nodes know each other's *identifier* and location,

they can independently execute the hash function to determine which node would be the coordinator. The coordinator then selects m nodes randomly (including itself), and broadcasts this list of m selected vote-participants to all group members. Because all m nodes know each other's identities, any node not following the protocol raises a flag as a potentially compromised node, and may get itself evicted when it is being evaluated as a target node. After m vote-participants for a target node are selected this way, each vote-participant independently votes for or against the target node by disseminating its vote to all group members. Vote authenticity is achieved via preloaded public keys. All group members know who the m vote-participants are, and based on votes received, can determine whether or not a target node is to be evicted.

For the attacker behavior, we consider the presence of smart attackers who will attempt to compromise other nodes with a variable rate depending on the number of compromised nodes in the system. In this paper, we consider the use of a *linear time attacker* function for modeling the attacker behavior, taking into account the possibility of collusion of compromised nodes in the system with the attack rate being linear to the attacker population. Voting-based IDS performs its function periodically. To counter smart attackers, the IDS detection interval is also adjusted dynamically in response to intrusion incidents that have been detected in the system. In this paper, we consider the use of a *linear periodic detection* function for IDS such that the detection rate increases linearly with the number of compromised nodes already detected by IDS.

A. Group Failure, and System Failure Definitions

We consider the *system lifetime* as the security-induced failure time of the mission-oriented GCS consisting of mobile groups in MANETs. We consider two separate system failure definitions for which we will analyze their effect on system lifetime:

- *System Failure Definition 1 (SF1)*, which is when the GCS fails when any mobile group fails; and
- *System Failure Definition 2 (SF2)*, which is when the GCS fails when all mobile groups fail.

In multi-hop MANETs, a GCS may contain multiple mobile groups at any given time because a mobile group may partition into two groups due to node mobility and failure, and any two groups may merge into one when they are close to each other. The first system failure definition (SF1) applies to the case in which a security failure of any mobile group risks the entire system, and causes the system to fail. For example, if the mission is to rescue military personnel by mobile groups, then any compromised mobile group will cause the entire rescue operation to fail. The second system failure definition (SF2) applies to the case in which as long as there is one mobile group available in the GCS, the mission continues. An example is to reach a certain destination for tactical operations by mobile groups. In this case, any mobile group can operate independently of other mobile groups, and the system fails only when all mobile groups fail. We will evaluate the effect of these two system failure definitions on the *MTTSF* of the system.

A mobile group in MANETs fails when one of two security failure conditions is true:

Condition 1 (C1): a compromised but undetected group member requests and subsequently obtains data using the group key. The mobile group is in a failure state because data have been leaked out to a compromised node, leading to the *loss of system integrity* [9].

Condition 2 (C2):more than 1/3 of group member nodes are compromised, but undetected by IDS. This failure condition follows the *Byzantine Failure* model [6] that if more than 1/3 of the member nodes are compromised, then the mobile group is compromised, resulting in the *loss of availability* [9] of system service. Note that, under the Byzantine failure model, a compromised node may send arbitrary messages to other group members to cause command inconsistency, and disrupt mission execution.

B. Network Connectivity

MANET environments may generate two connectivity scenarios: group nodes are connected within a single hop, forming a single group in the system without experiencing group merge or partition events; and group nodes are connected through multihops so that there are multiple groups in the system due to group partition/merge events because of node mobility or node failure. For the former scenario, where there is only a single group in the system, SF1 and SF2 (i.e., the two system failure definitions) are the same. We will consider both MANET connectivity scenarios in the paper, and see the effect of network connectivity on *MTTSF* of the GCS.

C. Reliability Metric

We use the system's mean time to security failure (*MTTSF*) to measure the system reliability of the mission-oriented GCS in MANETs. We will interchangeably call *MTTSF* the average system lifetime of the GCS.

- *MTTSF*: This metric indicates the lifetime of the GCS before it fails. A GCS fails when one mobile group fails, or when all mobile groups fail in the mission-oriented GCS, as defined by SF1 or SF2. On the other hand, a mobile group fails when either C1 or C2 is *true*. A lower *MTTSF* also implies a faster *loss of system integrity,* or *availability*. Therefore, our design goal is to maximize *MTTSF*.

III. Performance Model

We develop a mathematical model based on Stochastic Petri nets (SPN) [22], as shown in Fig. 1, to describe the behaviors of a mission-oriented GCS, instrumented with IDS to deal with insider attacks in MANETs. The performance model helps identify the optimal intrusion detection interval to maximize the system lifetime *MTTSF* of the GCS. We use SPN for reliability assessment because it provides a concise representation of the underlying Markov model, which potentially may contain tens of thousands of states. SPN models also allow general time distributions, rather than just exponential distributions, to be associated with event times if necessary.

The SPN model is constructed as follows.

- The SPN model tracks the behavior of a single mobile group as it evolves. This mobile group may be partitioned into two groups, and may merge with another mobile group

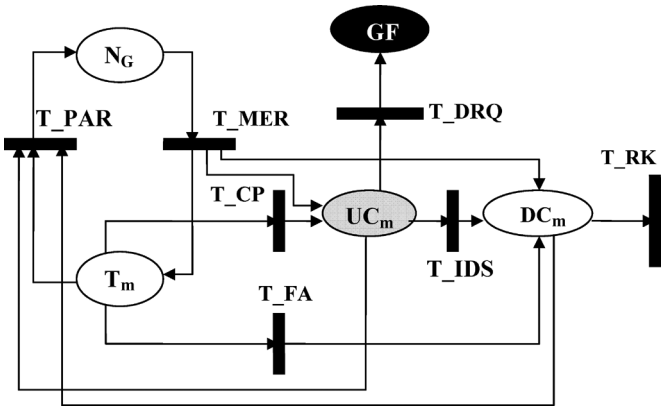

Fig. 1. The SPN model.

during its lifetime. We track trusted group members, compromised members undetected, and compromised members detected within this mobile group during its lifetime to understand its security and performance characteristics.

- The SPN model also tracks the number of mobile groups existing in the GCS during the system lifetime so we could decide if the GCS fails based on the system failure definition (SF1 or SF2).
- We use places to hold SPN tokens, representing head counts or nodes. Except for tokens held in place N_G, we use a token in the SPN model to represent a node in this mobile group. Initially, all N members are trusted in this mobile group, and put in place T_m as tokens. We use place N_G to hold the number of mobile groups existing in the system. Other places are used to hold nodes in this mobile group. Specifically, place T_m holds trusted member nodes, UC_m holds compromised nodes not yet detected by IDS, and DC_m holds compromised nodes that have been detected by IDS. The numbers of nodes held in places T_m, UC_m, and DC_m, represented by $mark(T_m)$, $mark(UC_m)$, and $mark(D_m)$, respectively, may be computed based on the number of groups existing in the system (obtained by $mark(N_G)$), which changes upon occurrences of group merge/partition events.
- We use transitions to model events. Specifically, T_MER, and T_PAR model group merge, or partition events, respectively; T_CP models a node being compromised; T_FA models a node being falsely identified by IDS as compromised; T_IDS models a compromised node being detected correctly by IDS; T_RK models rekeying; and T_DRQ models a data leak security failure due to C1. Firing a transition will change the state of the system. This event is represented by a redistribution of tokens in the SPN. For example, upon a group merge, or partition event, as indicated by firing T_MER, or T_PAR respectively, the number of groups is changed, so $mark(N_G)$ will decrement, or increment by 1 accordingly. When IDS detects a compromised node as indicated by firing T_IDS, the number of compromised nodes detected will be incremented by 1, so place DC_m will hold one more token. On the other hand, the number of undetected compromised nodes will be decremented by 1, so place UC_m will hold one less token.
- A transition is eligible to fire when the firing conditions associated with the event are met, including (a) its input places each must contain at least one token, and (b) the associated enabling guard function, if it exists, must return *true*. For example, T_CP is enabled to fire when there exist "good" nodes in the group; that is, place T_m holds at least one token, and the enabling function associated with T_CP returns *true*.
- In this mobile group, trusted members may become compromised because of insider attacks with a node-compromising rate θ. This event is modeled by associating transition T_CP with rate θ. See (6) for the parameterization of θ. Firing T_CP will move tokens one at a time (if they exist) from place T_m to place UC_m. Tokens in place UC_m represent compromised but undetected member nodes. We consider this mobile group as having experienced a security failure when data are leaked out to compromised but undetected members, i.e., due to C1. A compromised but undetected member will attempt to compromise data from other members in the mobile group. Because of the use of host-based IDS, a node will reply to such a request only if it could not identify the requesting node as compromised with the false negative probability $p1$. This event is modeled by associating transition T_DRQ with rate $p1 * \lambda_q * mark(UC_m)$, where λ_q is the expected query rate by a member. Firing transition T_DRQ will move a token into place GF, at which point we regard the mobile group as having experienced a security failure due to C1.
- A compromised node in place UC_m may be detected by IDS before it compromises data. The intrusion detection activity is modeled by the detection function with rate δ. See (7) for the parameterization of δ. Whether or not the damage has been done by a compromised node before the compromised node is detected depends on the relative magnitude of the node-compromising rate θ versus the IDS detection rate δ. When a compromised, undetected node is detected by IDS, transition T_IDS will fire, and a token in place UC_m will be moved to place DC_m. The transition rate of T_IDS is $mark(UC_m) * \delta * (1 - P_{fn})$, taking into consideration the false negative probability of voting-based IDS being used. Voting-based IDS can also incorrectly identify a trusted member node as compromised. This is modeled by moving a trusted member in place T_m to place DC_m after transition T_FA fires with rate $mark(T_m) * \delta * P_{fp}$. Note that voting-based IDS parameters P_{fn} and P_{fp}, are derived based on $p1$ and $p2$, the number of vote-participants m, and the current number of compromised nodes which may collude to disrupt the mobile group. The formulas for calculating P_{fn} and P_{fp} are given in (8) below. Here we note that if there is no token in UC_m, it means that there is no undetected bad node in the system, and consequently no new compromised node will be detected by IDS. This event is modeled by disabling (i.e., not firing) transition T_IDS when its input place UC_m contains no token.

- The mobile group being modeled is considered as having experienced a security failure if either one of the two security failure conditions, C1 or C2, is met. This situation is modeled by making the group enter an absorbing state when either C1 or C2 is *true*. In the SPN model, this condition is achieved by associating every transition in the SPN model with an enabling function that returns *false* (thus disabling the transition from firing) when either C1 or C2 is met, and returns *true* otherwise. For the SPN model, C1 is *true* when $mark(SF) > 0$, representing that data have been leaked out to compromised members; C2 is *true* when more than 1/3 of the member nodes have been compromised:

$$\frac{mark(UC_m)}{mark(T_m) + mark(UC_m)} > \frac{1}{3} \tag{1}$$

where $mark(UC_m)$ returns the number of compromised "bad" nodes in the mobile group, and $mark(T_m)$ returns the number of trusted "good" nodes in the mobile group.

A. Group Merge, and Partition

We obtain *group* merging/partitioning rates as follows. We first obtain the number of group merge and partition events by observing a multi-hop MANET simulator populated with mobile users with random way-point movements for a sufficiently long period of time. We next observe the sojourn time S_i in state i, i.e., when i groups are present in the system. Let $N_{nm,i}$, and $N_{np,i}$ be the numbers of group merge, or partition events observed in state i, respectively. Then the merging, and partitioning rates in state i, represented respectively by $\mu_{nm,i}$, and $\lambda_{np,i}$, are given by

$$\mu_{nm,i} = \frac{N_{nm,i}}{S_i}, \quad \lambda_{np,i} = \frac{N_{np,i}}{S_i} \tag{2}$$

We measure group merging/partitioning rates for the mobile user population ranging from 1 to N. We use the corresponding group merging/partitioning rates as transition rates to T_MER or T_PAR in the SPN model as the user population drops in the GCS as time progresses because of node eviction or failure. We observe that, when the node density is high, group merge is more likely to occur than group partition, thus resulting in a small number of large groups observed in the system. On the other hand, when the node density is low, the system is more likely to have a large number of small groups because group partition is more likely to occur than group merge. For the connectivity scenario in which all nodes are reachable within radio range, T_MER, and T_PAR in the SPN model of Fig. 1 are disabled to model the fact that there is only one mobile group in the GCS.

B. Calculation of MTTSF

MTTSF can be obtained by calculating the *mean time to absorption* (*MTTA*) of the SPN model through assigning proper rewards to states of the system [22]. We use a different reward assignment to calculate *MTTSF* under SF1 versus SF2. *MTTSF* under SF1 is calculated by assigning a reward of 1 to all states except for absorbing states in which C1 or C2 is met. We do this reward assignment because the system fails when any single group fails. Recall that the SPN model developed is for modeling the lifetime of a single group. On the other hand, *MTTSF* under SF2 is calculated by assigning a reward of

$$r_i = \left(\frac{1}{n} + \cdots + \frac{1}{1}\right) \tag{3}$$

to all states except for the absorbing states in which C1 or C2 is met. We do this assignment because the system fails when all groups fail. Thus, based on the concept of the *mean time to failure* of a *1-out-of-n* system [22] where n is the number of groups in the GCS given by $mark(N_G)$, we would accumulate a reward of $(1/n + \cdots + 1)$ instead of just 1 toward the system lifetime in those states in which the system is still alive.

After proper rewards to states are assigned as above, the *MTTSF* of the GCS can be calculated by the expected accumulated reward until absorption, defined as

$$E\left[Y(\infty)\right] = \sum_{i \in S}^{infty} r_i \int_o^{\infty} P_i(t)dt \tag{4}$$

where S denotes the set of all states except the absorbing states. For all i states, $r_i = 1$ under SF1, and r_i is given by (3) under SF2.

IV. Parameterization

To use the SPN model developed for performance analysis, we need to give model parameters proper values reflecting the operational and environmental conditions of the system. Below we describe this parameterization process for key model parameters.

- Transition rate of T_RK: This is the rekeying rate, the magnitude of which depends on the number of group members, N, because the amount of time used to generate a new key is linear with the number of nodes executing the key agreement protocol, GDH. Let T_{cm} be the time used to generate a new group key with N members. The reciprocal of T_{cm} is the transition rate of T_RK. Based on GDH, T_{cm} can be calculated by

$$if(N>1)\ T_{cm} = \frac{3b_{GDH}(N-1)}{BW} else\ T_{cm} = \frac{b_{GDH}}{BW} \tag{5}$$

where the number of current member nodes in the mobile group, N, is given by $mark(T_m) + mark(UC_m) \ldots$
- θ: This is the linear attacker function [6] that returns the rate at which "good" nodes will be compromised in the system. It is also the rate of transition T_CP, calculated by

$$\theta = \lambda_c \times m_c$$
$$m_c = \frac{mark(T_m) + mark(UC_m)}{mark(T_m)} \tag{6}$$

where m_c represents the *degree* of compromised nodes, given by the ratio of the number of group members over the number of "good" nodes in the same group. Note that the compromising rate (λ_c) may be obtained from design knowledge, or by first-order approximation from observing

TABLE I
MAIN PARAMETERS AND DEFAULT VALUES

Parameter	Value	Parameter	Value
λ	1/(60*60)	r	500 *m*
μ	1/(60*60*4)	σ	1/(60*60*32)
T_{IDS}	5 *s* – 1200 *sec*	BW	1 *Mbps*
λ_c	1/(60*60*12)	N_{init}	150 *nodes*
λ_q	1/(60*2)	δ/θ	Linear to m_d/m_c
$p1$, $p2$	1 %	m	3, 5, 7
b_{GDH}	64 *bits*	R	200 *m*

the number of compromised nodes over a time period based on past experiences.

- δ: This is the linear detection function that returns the rate at which IDS should be invoked, with its intensity adjusted linear to the cumulative number of compromised nodes that have been detected by IDS. It is computed as

$$\delta = \frac{1}{T_{IDS}} \times m_d$$
$$m_d = \frac{N_{init}}{mark(T_m) + mark(UC_m)} \tag{7}$$

where m_d represents the *degree* of nodes that have been detected by IDS, given by the total number of nodes initially in the system over the number of current nodes. The base intrusion detection interval T_{IDS} is a design parameter to be adjusted to maximize *MTTSF*.

- P_{fn}&P_{fp}: P_{fn} is the probability of false negatives, and P_{fp} is the probability of false positives in voting-based IDS. We parameterize them by (8) shown at the bottom of the page where p corresponds to $p1$, or $p2$ for respectively false negative, or false positive probability of host-based IDS installed in each node; $N_{majority}$ is the majority of m (e.g., $N_{majority} = 3$ if $m = 5$); $N_{good} = mark(T_m)$; and $N_{bad} = mark(UC_m)$. Here, P_{fn} is calculated through the number of ways by which m vote-participants are selected among good and bad nodes such that a compromised node is incorrectly diagnosed as a trusted good node, over the number of ways m vote-participants are selected among good and bad nodes. On the other hand, P_{fp} is calculated by the number of ways by which m vote-participants are selected among good and bad nodes such that a good node is incorrectly flagged as an anomaly, over the number of ways m vote-participants are selected among good and bad nodes. Equation (8) considers intrinsic defect of host-based IDS in each node, as well as collusion of compromised nodes in voting-based IDS, so a compromised participant can cast a negative vote against a healthy target node, and conversely can cast a positive vote for a malicious node.

V. NUMERICAL RESULTS, AND ANALYSIS

Below, we present numerical results obtained from evaluating the SPN model, following the parameterization process for assigning proper values to model parameters, as well as using default parameter values for other parameters as listed in Table I. The numerical results are obtained by defining a SPN model using SPNP [1] as a tool, and then evaluating the SPN model to compute *MTTSF* based on (4) after parameter values are given. In particular, we use $p1 = p2 = 1\%$ because in general less than 1% of false positive or false negative is considered acceptable. We report *MTTSF* of the GCS as described, versus the IDS interval under both system failure definitions (SF1, and SF2) in single-hop, or multi-hop MANET environments. We also report the sensitivity of *MTTSF* with respect to m, the number of vote-participants selected for performing majority voting in voting-based IDS, λ_q, the group communication rate, and λ_c, the base compromising rate. We have observed that *MTTSF* is insensitive to the group rekeying rate to transition T_RK because the group rekey rate obtained from (5) is at least an order of magnitude higher than λ_q, and several orders of magnitude higher than λ_c. Because the underlying model of the SPN model is a continuous-time Markov chain, any transition with a rate considerably higher than those associated with other transitions will take relatively very little time to complete. Consequently, T_RK has little impact on *MTTSF*.

Fig. 2 shows the effect of intrusion detection interval (T_{IDS}) on *MTTSF* as the number of vote-participants (m) in voting-

$$P_{fp}\ or\ P_{fn} = \sum_{i=0}^{m-N_{majority}} \left[\frac{C\begin{pmatrix} N_{bad} \\ N_{majority}+i \end{pmatrix} \times C\begin{pmatrix} N_{good} \\ m-(N_{majority}+i) \end{pmatrix}}{C\begin{pmatrix} N_{bad}+N_{good} \\ m \end{pmatrix}} \right]$$
$$+ \sum_{i=0}^{m-N_{majority}} \left[\frac{C\begin{pmatrix} N_{bad} \\ i \end{pmatrix} \times \sum_{j=N_{majority}-i}^{m-i} \left[C\begin{pmatrix} N_{good} \\ j \end{pmatrix} \times p^j \times C\begin{pmatrix} N_{good}-j \\ m-i-j \end{pmatrix} \times (1-p)^{(m-i-j)} \right]}{C\begin{pmatrix} N_{bad}+N_{good} \\ m \end{pmatrix}} \right] \tag{8}$$

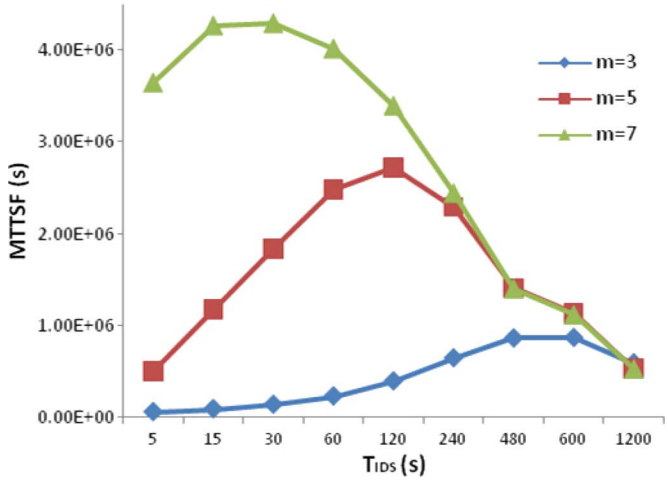

Fig. 2. Effect of T_{IDS} on *MTTSF* under varying m in single-hop MANETs.

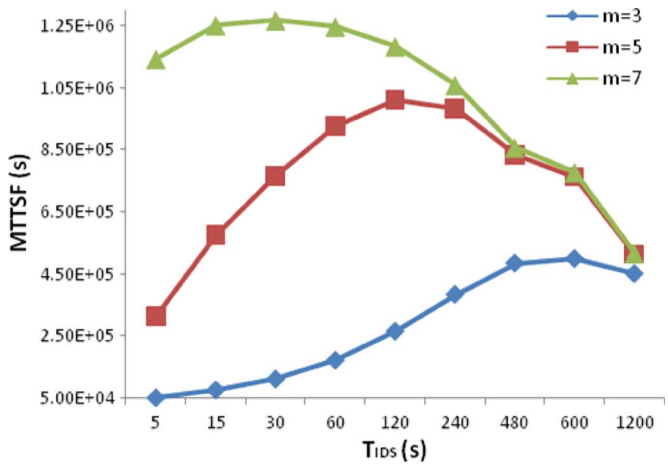

Fig. 3. Effect of T_{IDS} on *MTTSF* under varying m in multi-hop MANETs based on SF1.

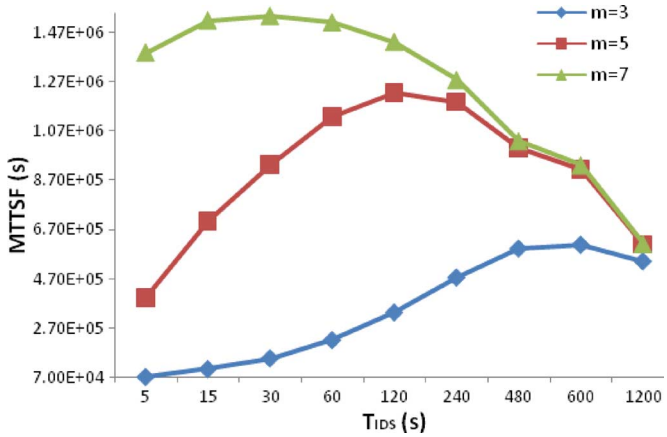

Fig. 4. Effect of T_{IDS} on *MTTSF* under varying m in multi-hop MANETs based on SF2.

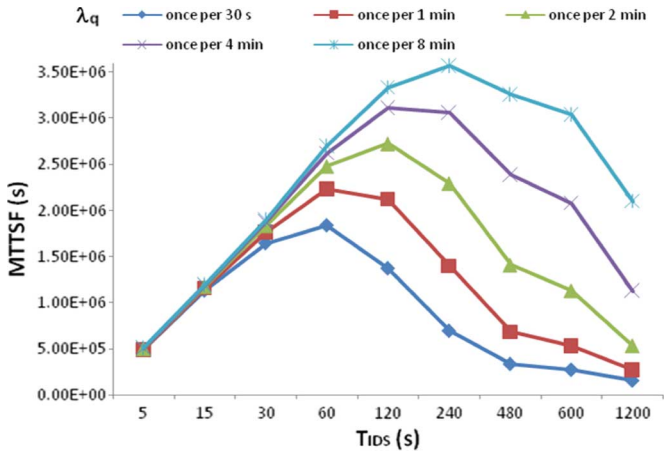

Fig. 5. Sensitivity of *MTTSF* with respect to λ_q in single-hop MANETs.

based IDS changes in single-hop MANETs in which only one mobile group exists in the GCS during the lifetime, with the system failure definition SF1 being equal to SF2. We see that there exists an optimal T_{IDS} that maximizes *MTTSF*. As T_{IDS} increases, *MTTSF* increases until its optimal point, and then *MTTSF* decreases after the optimal point. The reason for having increasing *MTTSF* as T_{IDS} increases initially is that triggering IDS too often has the effect of evicting nodes quickly in the system due to false positives, thus resulting in a quick system failure because of C2. Here, we note that negative effects of IDS are mostly due to false positives (diagnosing good nodes as bad nodes), and the effects are more pronounced when IDS is triggered more often. The reason for having decreasing *MTTSF* as T_{IDS} increases further past the optimal point is that, when IDS is not been triggering often enough, more compromised nodes will remain in the system, thus resulting in system failures mostly due to C1, and partly due to C2.

We also see from Fig. 2 the effect of m (the number of vote-participants in voting-based IDS) on *MTTSF*. When m is large, the false alarm probability $(P_{fp} + P_{fn})$ is low because more nodes will participate in the voting process, thus reducing the possibility of collusion by compromised nodes. Consequently, when m is large, we observe a high *MTTSF*. Conversely, when m is small, the false alarm probability is relatively large, resulting in a small *MTTSF*. This trend is generally true when the mobile user population is sufficiently high so that the probability of being able to find m nodes is sufficiently high. Lastly, we observe that a smaller m results in a large T_{IDS} being used to maximize *MTTSF* to offset the adverse effects of IDS with large false positives.

Figs. 3 and 4 show the effect of intrusion detection interval T_{IDS} on *MTTSF* as the number of vote-participants m varies in multi-hop MANETs for system failure definitions SF1, and SF2, respectively. Here, nodes are connected by multiple hops so that multiple groups exist in the system due to occurrences of group merge/partition events in the GCS. Similar to Fig. 2, we see from Figs. 3 and 4 that an optimal intrusion detection interval T_{IDS} exists to maximize *MTTSF*. Further, the optimal T_{IDS} value increases as m decreases. The same reasoning used for explaining these trends in Fig. 2 applies. We observe that *MTTSF* of the GCS in single-hop MANETs is comparatively higher than *MTTSF* of the same GCS in multi-hop MANETs under either system failure definition (SF1, or SF2). The reason is that when there are multiple groups in the system, the node density in each group tends to be small, given that the GCS is initially deployed with $N_{init} = 150$ users. Here we see the adverse

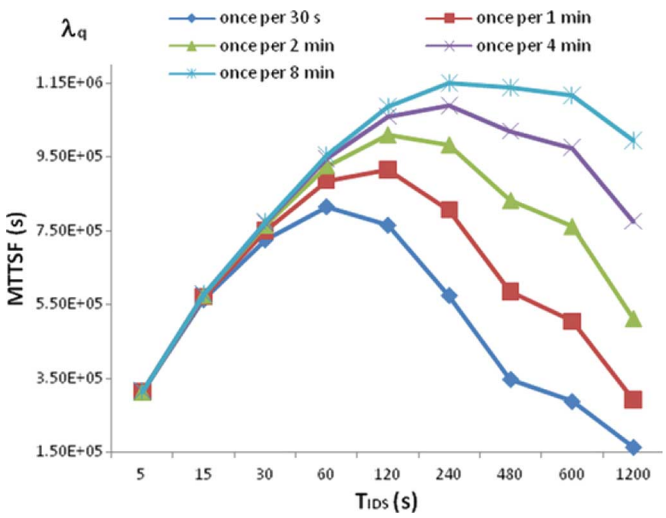

Fig. 6. Sensitivity of *MTTSF* with respect to λ_q in multi-hop MANETs based on SF1.

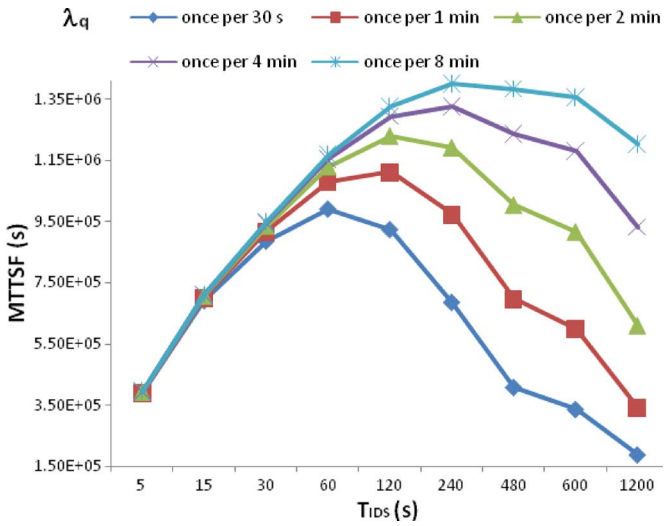

Fig. 7. Sensitivity of *MTTSF* with respect to λ_q in multi-hop MANETs based on SF2.

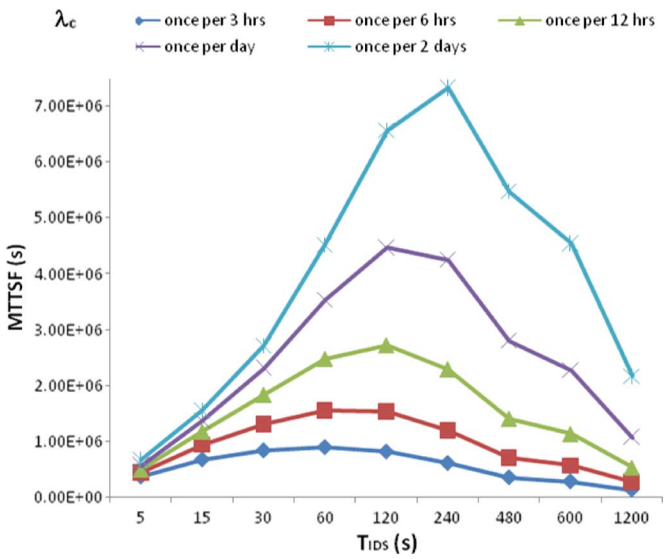

Fig. 8. Sensitivity of *MTTSF* with respect to λ_c in single-hop MANETs.

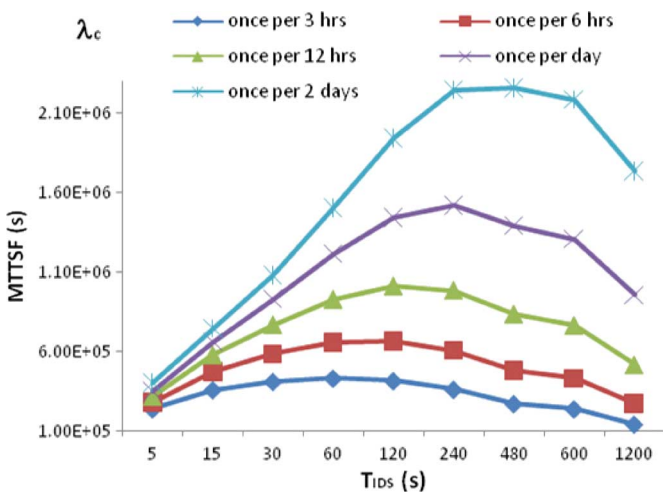

Fig. 9. Sensitivity of *MTTSF* with respect to λ_c in multi-hop MANETs based on SF1.

effect of breaking the system into multiple mobile groups on *MTTSF*. Lastly, we observe from Figs. 3 and 4 that the *MTTSF* of the system under SF2 is much higher than that of the system under SF1 because SF2 allows the mission to continue as long as one mobile group exists.

Below, we test the sensitivity of the results with respect to the group communication rate λ_q, and the base node compromising rate λ_c. Fig. 5 shows the sensitivity of *MTTSF* with respect to the group communication rate λ_q in single-hop MANETs. We observe that, when λ_q is low so the data-leak attack is not performed often, the positive effect of IDS is pronounced, leading to a high *MTTSF*. On the other hand, when λ_q is high so the data-leak attack is frequent, the negative effect of IDS is pronounced, so *MTTSF* is low. We also observe that the optimal T_{IDS} becomes smaller as λ_q increases because the system prefers removing compromised nodes as soon as possible so that compromised nodes would not have a chance to perform data-leak attacks. Another observation is that, when T_{IDS} is sufficiently small, e.g., $T_{IDS} < 60$ seconds, *MTTSF* remains about the same regardless of the magnitude of λ_q. This result is true because, when IDS is being invoked too frequently, the adverse effect of false positives dominates the positive effect of IDS.

Figs. 6 and 7 test the sensitivity of *MTTSF* with respect to the group communication rate (λ_q) in multi-hop MANETs based on SF1, and SF2, respectively. We see that there exists an optimal T_{IDS} under which *MTTSF* is maximized, and that the optimal point decreases as λ_q increases, exhibiting the same trend as in single-hop MANETs. Comparing single-hop MANETs versus multi-hop MANETs, however, we observe that the optimal T_{IDS} is smaller in single-hop MANETs under identical conditions. The reason is that single-hop MANETs tend to have more group members because all members are within one-hop radio range. Consequently, single-hop MANETs need to perform IDS more frequently to prevent potentially more compromised nodes from attacking the system, causing C1 or C2 to be violated. Comparing *MTTSF* in multi-hop MANETs based on SF1 and SF2, we observe that a higher *MTTSF* is obtained

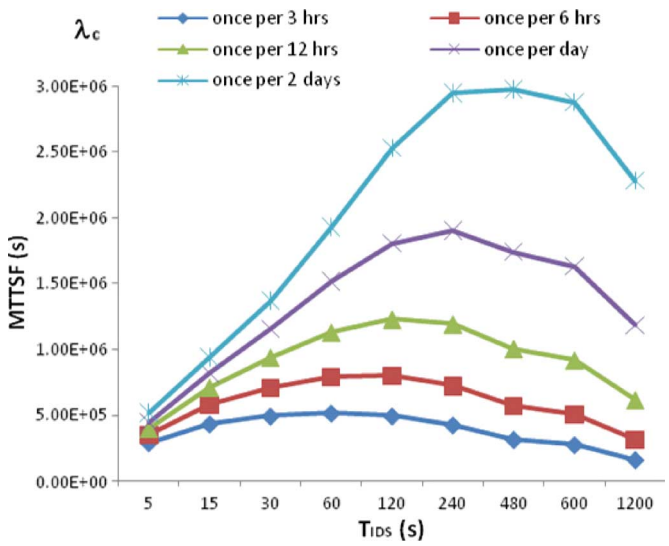

Fig. 10. Sensitivity of *MTTSF* with respect to λ_c in multi-hop MANETs based on SF2.

under SF2 because the system fails when all groups fail, as opposed to when one group fails.

Next, we test the sensitivity of *MTTSF* with respect to the base compromising rate λ_c in single-hop MANETs. Fig. 8 summarizes the results. We first observe that, as λ_c increases, *MTTSF* decreases because a higher λ_c will cause more compromised nodes to be present in the system. We also observe that the optimal T_{IDS} decreases as λ_c increases. This is because, when more compromised nodes exist, the system needs to execute IDS more frequently to maximize *MTTSF*. Finally, we observe that, when λ_c is low, the effect of T_{IDS} on *MTTSF* is especially pronounced. Thus, IDS is more effective when λ_c is sufficiently low.

Correspondingly, Figs. 9 and 10 summarize the sensitivity of *MTTSF* with respect to the compromising rate λ_c in multi-hop MANETs based on SF1, and SF2, respectively. The sensitivity result exhibited in Figs. 9 and 10 for multi-hop MANETs is remarkably similar in trend to that in Fig. 8 for single-hop MANETs. Comparing single-hop MANETs versus multi-hop MANETs, we observe two results: (a) single-hop MANETs have higher *MTTSF* because more members exist in single-hop MANETs, and (b) the optimal T_{IDS} is smaller in single-hop MANETs under identical conditions because the system tends to execute IDS more frequently when there are more members in a group. Comparing multi-hop MANETs under SF1 and SF2, we again observe a significantly higher *MTTSF* being obtained under SF2 due to the less stringent system failure definition for the GCS mission being executed.

VI. Applicability

In this paper, we developed mathematical models to analyze and reveal the optimal rate to execute intrusion detection to enhance the system reliability of group communication systems in mobile ad hoc networks, when given information regarding operational conditions, system failure definitions, and attacker behaviors. Our results indicate that the optimal intrusion detection interval T_{IDS} for maximizing the mean time to system failure (and hence for improving the system reliability) decreases as the number of vote participants m increases, as the node density or the group size increases, as the base compromising rate λ_c increases, and as the group communication rate λ_q increases. The analysis methodology developed is generally applicable, requiring only a modification to the model parameterization process to reflect changes in operational environments, system failure definitions, and attacker behaviors.

References

[1] G. Ciardo, R. M. Fricks, J. K. Muppala, and K. S. Trivedi, Department Electrical Engineering, Duke University, "SPNP Users Manual Version 6," 1999.

[2] H. Chan, V. D. Gligor, A. Perrig, and G. Muralidharan, "On the distribution and revocation of cryptographic keys in sensor networks," *IEEE Trans. Dependable and Secure Computing*, vol. 2, no. 3, pp. 233–247, July–Sept. 2005.

[3] Y. Chen and Q. Zhao, "On the lifetime of wireless sensor networks," *IEEE Communications Letters*, vol. 9, no. 11, pp. 976–978, Nov. 2005.

[4] M. Dacier, Y. Deswarte, and M. Kaâniche, Quantitative assessment of operational security: Models and tools Laboratory for Analysis and Architecture of Systems, Technical Report 96493, May 1996.

[5] Q. Dong, "Maximizing system lifetime in wireless sensor networks," in *4th Int'l Symposium on Information Processing in Sensor Networks (IPSN2005)*, April, 2005, pp. 13–19.

[6] F. C. Gärtner, Byzantine failures and security: Arbitrary is not (always) random Swiss Federal Institute of Technology (EPFL) School of Computer and Communication Sciences, Technical Report IC/2003/20, 2003.

[7] M. Esseghir and N. Bouabdallah, "Node density control for maximizing wireless sensor network lifetime," *Int'l Journal of Network Management*, vol. 18, no. 2, pp. 159–170, March 2008.

[8] E. Jonsson and T. Olovsson, "A quantitative model of the security intrusion process based on attacker behavior," *IEEE Trans. Software Engineering*, vol. 23, no. 4, pp. 235–245, April 1997.

[9] T. Karygiannis and L. Owens, *Wireless Network Security: 802.11, Bluetooth and Handheld Devices*. : National Institute of Standards and Technology (NIST), 2002, pp. 800–48, Special Publication.

[10] Z. Li and A. Das, "The utility of partial knowledge in behavior models: An evaluation for intrusion detection," *Int'l Journal of Network Security*, vol. 1, no. 3, pp. 138–146, 2005.

[11] Z. Li and B. Li, "Probabilistic power management for wireless ad hoc networks," *ACM Mobile Networks and Applications*, vol. 10, no. 5, pp. 771–782, Oct. 2005.

[12] X. Li, Y. R. Yang, M. G. Gouda, and S. S. Lam, "Batch rekeying for secure group communications," in *Proc. 10th Int'l Conf. on World Wide Web*, Hong Kong, May 2001, pp. 525–534.

[13] Y. Ma and J. H. Aylor, "System Lifetime Optimization for Heterogeneous Sensor Networks with a Hub-spoke Technology," *IEEE Trans. Mobile Computing*, vol. 3, no. 3, pp. 286–294, July/Aug. 2004.

[14] B. B. Madan, K. G. Popstojanova, K. Vaidyanathan, and K. S. Trivedi, "A method for modeling and quantifying the security attributes of intrusion tolerant systems," *Performance Evaluation*, vol. 56, no. 1–4, pp. 167–186, 2004.

[15] B. B. Madan, K. G. Popstojanova, K. Vaidyanathan, and K. S. Trivedi, "Modeling and quantification of security attributes of software systems," in *Int'l Conf. Dependable Systems and Networks*, Washington, D.C., June 2002, pp. 505–514.

[16] E. Melo and M. Liu, "Analysis of energy consumption and lifetime of heterogeneous wireless sensor networks," *IEEE Globecom*, pp. 21–25, 2002.

[17] D. M. Nicol, W. H. Sanders, and K. S. Trivedi, "Model-based evaluation: From dependability to security," *IEEE Trans. Dependability and Secure Computing*, vol. 1, no. 1, pp. 48–65, Jan.–March 2004.

[18] A. Patcha and J. M. Park, "A game theoretic formulation for intrusion detection in mobile ad hoc networks," *Int'l Journal of Network Security*, vol. 2, no. 2, pp. 131–137, 2006.

[19] A. Perrig and J. D. Tygar, *Secure Broadcast Communication in Wired and Wireless Networks*. : Kluwer Academic Publishers, 2002.

[20] S. Pillin, R. Mangharam, B. Bougard, L. Van der Perr, I. Moerman, R. Rajkumar, and F. Catthoor, "MEERA: Cross-layer methodology for energy efficient resource allocation in wireless networks," *IEEE Trans. Wireless Communications*, vol. 6, no. 2, pp. 617–618, Jan. 2008.

[21] K. G. Popstojanova, F. Wang, R. Wang, F. Gong, K. Vaidyanathan, K. S. Trivedi, and B. Muthusamy, "Characterizing Intrusion tolerant systems using a state transition model," in *Proc. the DARPA Information Survivability Conf. and Exposition*, June 2001, vol. 2, pp. 211–221.

[22] R. A. Sahner, K. S. Trivedi, and A. Puliafito, *Performance and Reliability Analysis of Computer Systems*. : Kluwer Academic Publishers, 1996.

[23] L. Sánchez-Miquel, N. Vesselinova-Vassileva, and F. Barcelü, "Energy and delay-constrained routing in mobile ad hoc networks: An initial approach," in *Proc. the 2nd ACM Int'l Workshop on Performance Evaluation of Wireless Ad hoc, Sensor, and Ubiquitous Networks*, Montreal, Quebec, Canada, Oct. 2005, pp. 262–263.

[24] C. Sengul and R. Kravets, "TITAN: On-demand topology management in ad hoc networks," *ACM SIGMOBILE Mobile Computing and Communication Review*, vol. 9, no. 1, pp. 77–82, Jan. 2005.

[25] M. Steiner, G. Tsudik, and M. Waidner, "Diffie-Hellman key distribution extended to group communication," in *Proc. 3rd ACM Conf. on Computer and Communications Security*, Jan. 1996, pp. 31–37.

[26] F. Stevens, T. Courtney, S. Singh, A. Agbaria, J. F. Meyer, W. H. Sanders, and P. Pal, "Model-based validation of an intrusion-tolerant information system," in *Proc. the 23rd Symposium Reliable Distributed Systems*, Oct. 2004, pp. 184–194.

[27] C. Tang and P. K. McKinley, "Energy optimization under informed mobility," *IEEE Trans. Parallel and Distributed Systems*, vol. 17, no. 9, pp. 947–962, Sep. 2006.

[28] D. Wang, D. W. Bharat, B. Madan, and K. S. Trivedi, "Security analysis of SITAR intrusion tolerance system," in *Proc. 2003 ACM Workshop on Survivable and Self-regenerative Systems*. Fairfax, VA: , Oct. 2003, pp. 23–32.

[29] C. Zhang, B. DeCleene, J. Kurose, and D. Towsley, "Comparison of inter-area rekeying algorithms for secure wireless group communications," *Performance Evaluation*, vol. 49, no. 1/4, pp. 1–20, 2002.

[30] Y. Zhang, W. Lee, and Y. A. Huang, "Intrusion detection techniques for mobile wireless networks," *Wireless Networks*, vol. 9, pp. 545–556, 2003.

[31] Q. Zhao and L. Tong, "Energy efficient of large-scale wireless networks: Proactive versus reactive networking," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 5, pp. 1100–1112, May 2005.

Jin-Hee Cho (S'06–M'08) received her BA from Ewha Woman's University, and MA from Washington University in St. Louis, MO in 1997, and 1999 respectively. She also received her MS, and PhD in Computer Science from Virginia Tech in 2004, and 2008 respectively. She received an IREAN fellowship through the NSF IGERT program during her Ph.D. study. Currently she is a postdoctoral research fellow in Computational and Information Sciences Directorate, U.S. Army Research Laboratory, Adelphi, MD through the ARL/ORAU postdoctoral fellowship program. She received a best paper award in *The 2009 IEEE/IFIP International Symposium on Trusted Computing and Communications (Trustcom09)*, Vancouver, Canada. Her research interests include wireless mobile networks, mobile ad hoc networks, sensor networks, secure group communications, group key management, network security, intrusion detection, performance analysis, trust management, cognitive networks, social networks, and dynamic public key management. Dr. Cho is a member of the IEEE, and ACM.

Ing-Ray Chen (M'89) received the BS degree from the National Taiwan University, Taipei, Taiwan, and the MS and PhD degrees in computer science from the University of Houston. He is program director and professor in the Department of Computer Science at Virginia Tech. His research interests include mobile computing, security, pervasive computing, multimedia, distributed systems, real-time intelligent systems, and reliability and performance analysis. Dr. Chen has served on the program committee of numerous conferences in his research areas. He was an associate editor for IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING during 2000–2004, and currently serves as an editor for The Computer Journal, Wireless Communications and Mobile Computing, Wireless Personal Communications, Security and Communication Networks, and International Journal on Artificial Intelligence Tools. Dr. Chen is a member of the IEEE/CS, and ACM.

Phu-Gui Feng received her BS, and MS degree in computer science from George Mason University, Virginia. She is a Lead Software Engineer at Mitre Corporation. Currently she is working toward her PhD degree in Computer Science at Virginia Tech. Her research interests include computer networks, security, and service-oriented architectures.