Investigation of Performance-Security Tradeoff in Robotic Mobile Wireless Ad hoc Networks (RANETs) using Stochastic Petri Nets

Muhammad Jawad Ikram
University of Bradford, UK

Kashif Ahmad
University of Engineering & Technology, Peshawar, Pakistan

ABSTRACT

This paper presents a comprehensive review of performance-security trade-off based on RANETs. It is suggested that stochastic Petri nets (SPNs) are the best choice to investigate performance-security trade-off in RANETs. In the context of RANETs, a mathematical model that is based on SPNs is analysed to investigate performance-security trade-off. Security is assessed in terms of mean time to security failure (MTTSF) and performance is assessed in terms of service response time (R). The main objective is to find optimal settings that includes the best intrusion detection interval and best batch rekey interval under which mean time to security failure is maximized while satisfying performance requirement in terms of system response time.

Keywords

Mobile ad hoc networks (MANETs), robotic mobile wireless ad hoc networks (RANETs), queueing network models (QNMs), Petri nets, Stochastic Petri nets (SPN), intrusion detection system (IDS), rekeying.

1. INTRODUCTION

Performance and security are two of the main aspects of a system that should be kept under consideration during the design, development, tuning and upgrading of RANETs [3]. Performance of RANETs or any general computer network can be measured in terms of the standard metrics *throughput, packet loss probability, end-to-end delay* [4], *average number of hops, optimal hops and routing overhead* ([c.f. 5]). On the other hand there exists no standard metrics to measure security but it can be measured in terms of reliability metrics such as *mean time between security incidents, mean time to incident discovery, and mean time to incident recovery* as proposed by Wolter [1].

A situation in which one quality or feature of something is lost in return for gaining another quality or feature is called *trade-off* [1]. The performance-security *trade-off* means that both performance and security can be measured together and if we want to improve one, we have to pay in terms of the other. Encryption-decryption and security protocols cost extra computing resources. Security of a system can be measured by considering indirect metrics such as computational cost of security methods. Both performance and security can be quantified by means of stochastic models e.g. Queueing Network Model (QNM), Markov Chains Models and Petri Nets Models.

The trade-off between performance and security can be best studied by using a Petri net model. The advantage of Petri nets over queueing network model (QNM) is that in Petri nets, both performance and security can be considered explicitly [1]. From the Petri net model, the combined performance-security metrics can be formulated, from which the *trade-off* between both can be studied. It is shown that system parameters can be found that optimize both performance and security together [1].

This paper is organised as follows. An overview of mobile ad hoc networks (MANETs) and RANETs, various rekeying algorithms, IDS techniques and modelling aspects is presented in Section 2. In section 3, Performance-Security tradeoff is explored in depth, section 3 also reviews alternative SPN models, which may be used for the performance related security evaluation and prediction of RANETs. Section 4 presents parameterization of the whole work. In section 5 performance-security metrics are assessed. Numerical analysis, results and a discussion associated with other important aspects of RANETs follow in Section 6. Finally, the whole work is concluded in section 7.

2. BACKGROUND

This section exploits the compatibility of MANETs and RANETs and provides an overview security attacks in RANETs, rekeying algorithms and IDS techniques.

2.1 MANETs

MANET can be defined as a type of network in which there is no central administration and consists of mobile nodes that use a wireless interface to send packet data [2]. In other words, MANETs can be defined as a collection of two or more devices equipped with wireless communications and networking capability which is self-organizing and adaptive [4]. The network can be formed on the fly. There is no formal infrastructure and the nodes communicate in a multi-hop fashion. Since the nodes can move arbitrarily, so, the topology is dynamic and support multi-hop paths. MANET is simply an autonomous system of mobile nodes.

2.2 RANETs

As stated in [6] "at low cost solutions for wireless communication, robots should be developed to successfully perform cooperative work and have the capability to construct a network". Like all other emerging technologies robots also have become more robust and more intelligent and more power-efficient. Robots are needed to perform the teamwork efficiently. Robots should be able of doing cooperative work and should have the capability of to construct a network. Robots are specially needed in situation in which human presence is dangerous, for example nuclear power processing and rescue mission etc. [7]. Wireless communications provide cost effective solutions for robot to cooperate more efficiently as given in [6].

2.3 Why MANETs for RANETs?

Robots are developed to become more intelligent, robust and more power efficient. During critical mission like military operations and other dangerous environments where humans cannot go directly, an effective team work amongst robots is highly desired. Effective team work can be achieved by developing an efficient group communication system (GCS) of robots. Robots are most likely equipped with only low power wireless transceivers with short range, which although prevents direct communications with data collection points, nevertheless it sufficient to allow them to communicate with close neighbours. MANETs seems to be the most suitable platform for developing such an efficient system because there is no centralized control, and thus providing robustness against single point failures. Optimal broadcasting/multicasting methods may also be adopted in RANETs, leading into performance enhancement (c.f., [9], [10]).

2.4 Security Attacks in RANETs

Ad hoc networks are more exposed to security attacks as they have no strong line of defence [11]. Two types of security attacks are expected in ad hoc networks: insider attacks and outsider attacks. Outsider attacks come from outside of the network, for example if an external intruder attempts to gain unauthorized access to the group communication in the system. These attacks can be controlled by prevention methods like authentication and encryption. Insider attacks come from trusted members who become compromised due to some reasons and they can share the group key with some outsider attackers to break the security of the system. For controlling insider attacks, intrusion detection system (IDS) methods are developed to detect compromised nodes and evict them from group formation to achieve better security [11].

2.5 Rekeying Protocols for ad hoc Networks

Due to security attacks, the system may go to security failure state. The system can be recovered by performing a rekey operation. For rekeying, there exist a number of algorithms as proposed in [12, 13, 14]. The simplest rekeying algorithm is proposed in [14], i.e. *individual rekeying*. In [13], *batch rekeying* and *interval-based* distributed rekeying algorithm are proposed to achieve better rekeying for dynamic peer groups. In recent times, threshold-based periodic batch rekeying algorithms are proposed that are extremely useful to explore the trade-off between performance and security with the objective of identifying the best batch rekey interval [14]. On one hand, various rekeying algorithms provide defence against outsider attacks. On the other hand, the use of IDS methods provide defence against insider attacks to ensure high survivability as required in a secure, mission-critical group communication [8]. We consider three rekeying protocols for secure group communication between ad hoc nodes, which are as follow;

Individual Rekeying: In this technique, a CKA [11] rekeying is performed each time after a robot join or leave the system, or if a compromised node is removed from the system [8].

Trusted And Untrusted Double Threshold-based rekeying with CKA (TAUDT-C): As the name suggests, this is a threshold-based rekeying technique, which has thresholds (k_1, k_2), whenever these thresholds are reached, a CKA [11, 14] rekeying is performed [8]. Where, k_1= the number of requests from trusted join nodes plus trusted leave nodes, k_2= the number of requests due to evictions for the nodes detected by IDS as compromised

Join And Leave Doubled Threshold-based rekeying with CKA (JALDT-C): This is also a double threshold-based rekeying algorithm, which has thresholds (k_1, k_2), whenever these thresholds are reached, a CKA rekeying is performed [8]. k_1= the number of requests from trusted join nodes., k_2= the number of requests from trusted leave nodes plus the number of requests due to evictions for the nodes detected by IDS as compromised.

TAUDT-C and *JAUDT-C* are extensions of *JAUDT* and *TAUDT*, respectively [11, 14]. Both these protocols try to remove chances of single point failure in ad hoc networks by utilizing a CKA for distributed control. GDH.3 protocol [14] is considered as the CKA protocol for secret key generation.

2.6 Intrusion Detection System techniques for ad hoc Networks

We consider two types of Intrusion Detection System (IDS) protocols for secure group communication between ad hoc nodes, which are as follow;

Host-based IDS: In host-based IDS, a local detection is performed by each node (robot) to know whether a neighbouring node is compromised or not? This type of IDS can be implemented by using standard IDS techniques such as signature-based detection or anomaly detection [15]. In this technique, the neighbouring nodes are evaluated on the basis of information collected, that is mostly route-related and traffic-related [15]. Host-based IDS is characterized by two parameters, i.e. false negative probability (p_1) and false positive probability (p_2).

Voting-based IDS: Voting-based IDS that provide robustness against collusion. In voting-based IDS, a voting is performed by *m* vote participants, against a periodically selected node, called target node [15]. If the majority of vote goes against the target, then the target node would be evicted from the system. Voting-based IDS is characterized by two parameters, called false negative probability (P_{fn}) and false positive probability (P_{fp}). These two probabilities are calculated on the basis of (a) host-based false negative probability (p_1) and false positive probability (p_2); (b) the number of vote-participants (m) and (c) estimate to the current number of compromised nodes.

In voting-based IDS, each node determines its vote based on host-based IDS as it is entirely distributed. The eviction process is performed periodically. *m* vote-participants are selected such that each node periodically exchanges it routing information, location and id with all its neighbouring nodes. All the neighbours of a target node are candidates as vote-participants. A node with the smallest *id* elects itself as a *coordinator* and elects other *m* vote-participants (including itself). The *coordinator* then broadcast the list of *m* selected vote-participants to all the group members. Once the vote-participants are selected, each vote-participant cast its vote independently for or against a target node.

2.7 Stochastic Petri Nets Model

Petri nets are a proper notation designed for modelling concurrency, causality and conflict [19]. A Petri net is a bipartite graph that gives the formalism an easier intuitive interpretation than the Markov process, particularly, for small or moderately sized models [19]. Petri Net is a four- tuple i.e. PN = <P, T, I, O>. It is described as follow [19];

- P: a finite set of places, $\{P_1, P_2, ..., P_n\}$
- T: a finite set of transitions, $\{ T_1, T_2, ..., T_n\}$
- I: an input function, $(T \times P) \longrightarrow \{0, 1\}$
- O: an output function, $(T \times P) \longrightarrow \{0, 1\}$
- M_0: an initial marking, $P \longrightarrow \mathrm{N}$
- $<P, T, I, O, M_0>$ -- a marked Petri net

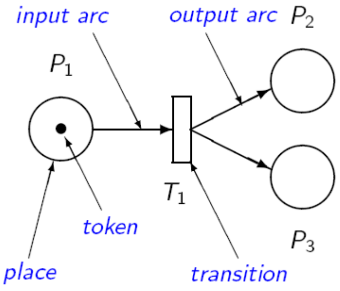

Fig 1: Anatomy of Petri Nets

In the early 1980s, stochastic Petri nets (SPN) come forward as a modelling formalism for performance analysis. Exponentially distributed delay is associated with the firing of each transition in SPN [19]. The delay happens between when the transition becomes enabled and when it fires. The instantaneous firing only occurs if the transition remains enabled all over the delay period. Marking of a place, e.g. for place P_1 in figure 1, is generally represented by $M(P_1)=1$, which means that there is a single token in place P_1.

3. PERFORMANCE-SECURITY TRADEOFF IN RANETs

We present a model based evaluation of the performance-security trade-off in RANETs as presented by Cho et al [8] for MANETS. Security is measured in terms of *mean time to security failure (MTTSF)* while performance is measured in terms of *service response time (R)*. The design objective is to maximize *MTTSF* and minimize *R*, and also to identify the best intrusion detection interval and best batch rekey interval at the same time. We consider a system in which group-communication is observed between a group of nodes in RANETs. All the nodes are robots and they are communicating in a group to accomplish an assigned mission, for example in military battlefield situations, where very high security and better performance is required. All Robots are working in coordination and there is no centralized control. A good performance and at the same time high security is required to accomplish the mission successfully. For security purposes, particularly, for avoiding outsider attacks, all the robots share a secret security key (group key) for communicating with each other. To maintain confidentiality and secrecy, the group key is rekeyed after every change of membership event.

3.1 Group Communication System of Robots

In this section some assumption are made in order to set a baseline for the proposed Stochastic Petri Net (SPN) model. It is assumed that the group communication is in a wireless ad hoc environment without any centralized control. All the nodes in the group communication system (GCS) are robots and are preloaded with public/private key pairs for authentication purposes. Robots can *join* the group only after authorization. This means that only trusted members can join the group. In contrast a *leave* can be either trusted or untrusted. Trusted *leave* means that if a member voluntary *leave* the group. Untrusted *leave* is caused by eviction of a detected compromised node. Robots may get compromised due to insider attacks or outsider attacks. To provide better security, there is an Intrusion Detection System (IDS), whose job is to evict compromised Robots. Evicted nodes cannot re-enter the group. Sometimes the IDS may not be able to detect a compromised node with a *false negative* probability, and may erroneously flag a correct host as compromised (false positive). IDS is preinstalled in every node to perform intrusion detection activities. Initially, the system performs host-based IDS to evict suspicious nodes. The system further performs voting-based IDS to alleviate collusion. It is assumed that *view synchrony* is guaranteed [16] in the GCS, which ensures that messages are delivered reliably and in proper order under the same group membership view. Only group members are allowed to communicate with each other. Communication between the group is encrypted by a shared group key. In fact, group-membership is equivalent to the knowledge of the shared group key. In order to avoid compromised nodes from accessing the group communication, a rekeying operation is required each time a node is evicted.

All the robots in the group are assumed to be spread over an area (A). It is further assumed that the occurrence of trusted *join*, trusted *leave* and data packets issued by a robot for group communication is according to exponential distribution with rates λ, μ and λ_q respectively. In order to realize distributed key management in ad hoc networks, it is assumed that the time to perform rekeying operation due to *join* or *leave* is measured based on GDH.3 protocol, proposed in [14]. The behaviour of the attacker is modelled with a *linear time attacker* function. Like the attacker behaviour *linear periodic detection* function is used to model IDS activities. On one hand ad hoc networks are resource-constrained and on the other hand there is rekeying overhead in terms of communication cost incurred due to *join/leave/eviction* requests, so, in order to alleviate this, batch rekeying is utilized [1].

It can be concluded from the discussion that performance of the system is influenced by join and leave rates as well as by the rekeying rate while security is influenced by the rate of nodes becoming compromised and detected as well as by the quality of the Intrusion Detection System [8]. The quality of the IDS is specified by false-positive and false-negative probabilities. The rekeying rate is specified by the communication time for broadcasting the rekeying message. Rekeying depends on the trigger conditions reflecting the rekeying threshold. The probabilities of false negatives and false positives are specified by the number of uncompromised and compromised, but undetected nodes.

3.2 Performance-Security Metrics for RANETs

Performance is measured as the response time for messages transmitted within the group, averaged over the total lifetime of the system. Security is defined as the Mean Time To Security Failure (MTTSF) such that the mean time until an attacker gains access to group communication or until the system becomes unavailable. The performance-security metrics can be summarized as follow;

Mean Time to Security Failure (MTTSF): This is a security metric that refers to the system lifetime before the system reaches the security failure state. A security failure state is reached when either condition 1 or condition 2 (stated above) is true.

Service Response Time (R): This is a performance metric that indicate mean response time per group communication operation. Every *join/leave/eviction* and IDS activities have an effect on the *system response time*.

Thus, the performance versus security trade-off can be studied and results can be obtained by varying the eviction thresholds and the IDS intervals. The results obtained by Cho et al. explain distinctive optima both in *MTTSF* and the *system response time*. In the light of these results, optimal parameters can be selected for the system.

3.3 Performance-Security Model

The mathematical model shown in figure 2 is used to study performance-security tradeoff in GCS of robots in which IDS is used to deal with insider attacks and batch rekeying is used to deal with outsider attacks. The design objective is determine optimal settings such that to maximize *MTTSF* and minimize *R* both at the same instant. In the beginning all nodes are trusted nodes and thus all tokens are placed at T_m. Afterwards, with some probability, nodes may either become compromised or with some other probability, the Intrusion Detection System (IDS) may erroneously detect that they have been compromised (false positive). Compromised nodes may get unauthorized access to data; that may lead the system to security failure state (SF). This event is modelled by transition *T_DRQ1*. Compromised nodes are evicted from the system by performing a rekeying operation based on the rekeying algorithms given section 2.5. The rekeying operation resets the system back to secure state. Note that rekeying is performed after every join/leave/eviction request. The join and leave events are modelled by transition *T_TJ* and *T_TJ*, respectively. The transition *T_RK* models rekeying operation. The transitions *T_FA* models the event of falsely detect compromised nodes in the system. Falsely detected compromised nodes are placed in place FDC_m. In this case the node is still available for group communication. The node is evicted from the group by the next rekeying operation that is modelled by the firing of the *T_RK* transition. A node may become compromised that may then be detected by the IDS and thus be evicted from the group communication by rekeying. This event is modelled by transitions *T_IDS*. Detected compromised nodes are placed at place DC_m. The detected compromised members may also request for unauthorized access of data, which causes security failure. This event is modelled by transition *T_DRQ2*. System security failure state is reached, because of compromised members either detected by IDS or not, gain access to the group communication. This event is modelled by transition *T_DRQ1* and *T_DRQ2* that moves the system to the absorbing state *SF*. Note that the join/leave requests has no effect on the system security, but have an influence on the performance, because rekeying operations are need after join and leave request.

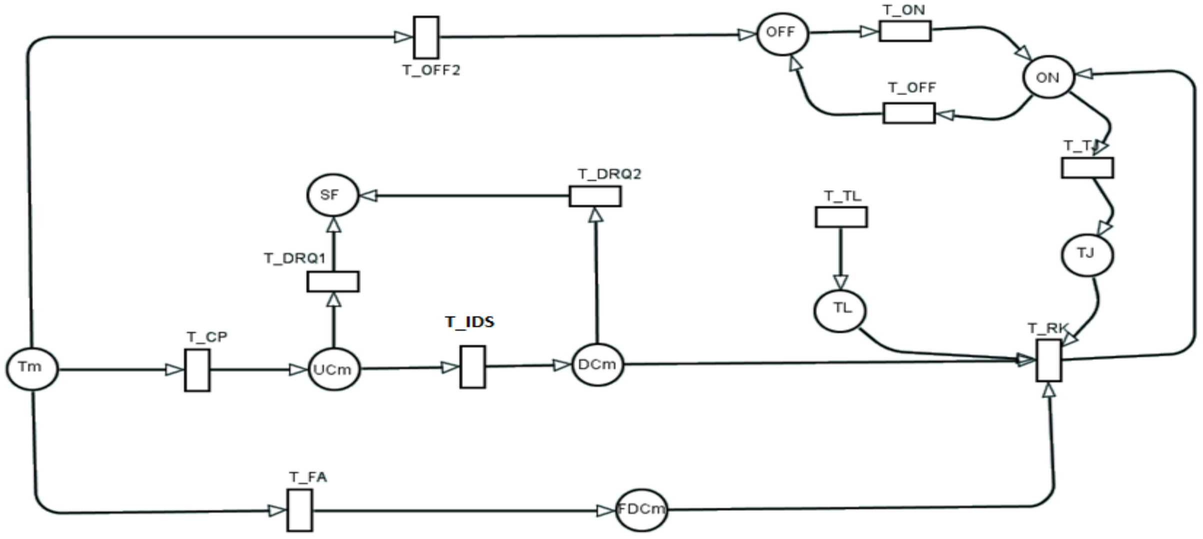

Fig 2: SPN model for Performance and Security in RANETs

3.4 Modelling Mobility in RANETs using Gated Queue

In order to capture mobility in RANETs, a gated queue with ON and OFF states is added to the proposed model of Cho et al [8]. The underlying concept of a gated queue is that a robot that is not reachable should be considered in OFF state and vice versa. Trusted members can only take part in group communication if they are in the coverage area. Due to some reasons, some of the nodes may go outside the of the coverage area with some probability, in which case they will not be able to access group communication. If nodes are no more in the coverage area, they are considered to be in *OFF* state for some time. This event is modelled by transition *T_OFF2*. Nodes that are not reachable hold by place *OFF*. These unreachable nodes can come to the coverage area again with some probability. This event is modelled by transition *T_ON*. Nodes that are reachable are hold by place *ON*. With some probability, these reachable nodes can either join the group or can go out of the coverage area again. A node must be reachable (in *ON* place) to join the group. In case of joining, rekeying is performed as usual. Evicted nodes my re-join the system, to model this, there is an arc drawn from transition *T_RK* to the *ON* place. It means that after leaving, the nodes may still be in the coverage area and if they want to re-join the group, rekeying is performed as usual. *ON* place is like a depository, from where nodes may enter join the group.

3.5 Security Failure State

Cho et al [18] define two security failure scenarios in exploring the performance versus security trade-off. In the first scenario, a compromised node gain access to the group communication. In the second scenario, very few users are left and group communication becomes impossible. The system reaches security failure states if one of the following conditions occurs;

Condition 1: The first security failure may occur either because a compromised node has not been detected by the IDS, or because it has been detected but has not been removed yet, which may lead to data leak-out to a compromised node.

Condition 2: The second security failure occurs if more than one-third (1/3) of the member robots are detected as compromised nodes by IDS. Byzantine failure model [18] is considered to model the failure condition.

Note that security of the system depends on the choices of thresholds in the rekeying algorithm and on the quality of the IDS.

4. PARAMETERIZATION

There are total 7 places in the given model that classify nodes (robots). Transitions are used to model events. A token in the SPN model represents a node in the system and the number of tokens at a place gives the total number of nodes in a particular place. Each place and transition holds different type of nodes and describe different event respectively, as describe below; Nodes that are trusted or correct are hold by place T_m.

- Nodes may become compromised due to insider or outsider attacks and may not be detected by the IDS; such nodes are placed in place UC_m, which simply means compromised but undetected nodes.
- IDS may falsely diagnose correct nodes as compromised nodes; the place FDC_m holds such nodes.
- Nodes that are compromised and also detected by IDS are placed in place DC_m.
- The places *TJ* and *TL* hold the nodes that have generated a join and leave request respectively.
- The place SF shows the security failure state. Whenever M(SF) > 0, security failure occurs and the system becomes insecure.
- All transitions are timed transitions. A triggering condition is also associated with a transition, which models the specific condition under which an event would occur. The triggering conditions and rates of the transitions are as follow;
- The triggering condition of *T_RK* depends upon the batch rekeying technique used. For *individual rekeying, T_RK* is triggered if the following condition holds.
  If M(TJ) >= 1 OR M(TL) >= 1 OR M (FDC_m) >=1 OR M(TJ) >= 1
- For *TAUDT-C rekeying*, *T_RK* is triggered if the following condition holds.
  If (M(TJ) + M(TL)) reaches k_1 OR (M(FDC_m) + M(DC_m)) reaches k_2
- For *JALDT-C rekeying*, *T_RK* is triggered if the following condition holds.
  If M(TJ) reaches k_1 OR (M(TL) + M(FDC_m) + M(DC_m)) reaches k_2
  Where k_1 and k_2 are two predefined thresholds.
- The rate of transition *T_RK* is 1/T_{cm};
  Where T_{cm} is the communication time required to broadcast a rekeying message. T_{cm} is calculated based on GDH.3 protocol as given below [44];

$$T_{cm} = \begin{cases} \frac{Nb_{GDH}(2H+1)-b_{GDH}(H+2)}{BW} & for\ N > 1 \\ \frac{b_{GDH}}{BW} & otherwise \end{cases}$$

  Where N = M(T_m) + M(UC_m), i.e. the number of current active nodes in the system, b_{GDH} = the length of an intermediate value, BW= bandwidth in Mbps, H = the number of hops between any two nodes
- Due to insider attacks, correct nodes may become compromised. The attacker behaviour is modelled by a *linear time attacker* function with rate $A(M_c)$ [18].
- The rate of *T_CP* is $A(m_c)$, and $A(m_c) = \lambda_c\ x\ m_c$
  Where λ_c = base compromising rate, m_c = the degree of current compromised nodes in the system, it can be calculates as follow; $m_c = \frac{M(UC_m)+M(T_m)}{M(T_m)}$. In simple words, we can say that m_c is the ratio of current active nodes (N) to the number of good nodes in the system.
- The system reaches the security failure state due to condition 1 (as stated in section 3.5) when undetected compromised nodes gain unauthorized access of data. This event is modelled by transition *T_DRQ1*.
- The rate of transition *T_DRQ1* is $p_1\ x\ \lambda_q\ x\ M(UC_m)$
  Where p_1 = host-based false negative probability, λ_q= data packets issued by a node for group communication.
- The undetected compromised nodes are detected by the IDS. This event is modelled by the transition *T*_IDS. The IDS detection rate is modelled by *linear time detection* function with detection rate $D(m_d)$ [18].
- For *voting-based IDS*, the rate of transition *T_IDS* is $M(UC_m)\ x\ D(m_d)\ x\ (1\text{-}P_{fn})$
  Where $D(m_d)$ = detection rate (the rate at which IDS is invoked)
  $D(m_d) = m_d/T_{IDS}$, Where T_{IDS} = base intrusion detection interval
  m_d = degree of nodes detected by IDS, it is given by; $m_d = \frac{N_{init}}{N} = \frac{N_{init}}{M(UC_m)+M(T_m)}$
  Where N_{init} indicates the initial number of nodes in the system, P_{fn} = voting-based false negative probability. Note that $P_{fn}$and $P_{fp}$are calculated using the host-based false negative *(p_1)* probability and false positive probability *(p_2)* respectively. The

equation for P_{fn}or $P_{fp}$is as follow [14]; $P_{fn} or P_{fp} =$

$$\sum_{i=0}^{m-\left\lceil\frac{m}{2}\right\rceil}\left[\frac{\binom{M(UC_m)}{\left\lceil\frac{m}{2}\right\rceil+i}\times\binom{M(T_m)}{m-\left(\left\lceil\frac{m}{2}\right\rceil+i\right)}}{\binom{M(T_m)+M(UC_m)}{m}}\right]+$$

$$\sum_{i=o}^{m-\left\lceil\frac{m}{2}\right\rceil}\left[\frac{\binom{M(UC_m)}{i}\times\sum_{j=\left\lceil\frac{m}{2}\right\rceil-i}^{m-i}\left[\binom{M(T_m)}{j}\times(p)^j\times\binom{M(T_m)-j}{m-i-j}\times(1-p)^{m-i-j}\right]}{\left(\binom{M(T_m)+M(UC_m)}{m}\right)}\right]$$

Where m = the number of voting participants, $p = p_1$ for P_{fn}, and p_2 for P_{fp}

- Correct or trusted nodes may erroneously be detected as compromised nodes with false positive probability. This event is modelled by transition *T_FA*. The rate of transition *T_FA* is $M(T_m)$ *x* $D(m_d)$ *x* P_{fp}, Where $D(m_d)$ and P_{fp} are calculated above.
- The system again reaches the security failure state due to condition 1 (as stated in section 3.5) if detected compromised nodes gain unauthorized access of data. This event is modelled by transition *T_DRQ2*. The rate of transition *T_DRQ1* is p_1 *x* λ_q *x* $M(DC_m)$. Where p_1 = host-based false negative probability, λ_q= data packets issued by a node for group communication
- New nodes may join the group communication system. This event is modelled by transition *T_TJ*. The rate of transition *T_TJ* is given by λ.
- Leaving event is modelled by transition *T_TL*. The rate of transition *T_TL* is given by µ.
- Security failure is experienced if either condition 1 is true or condition 2 is true. Condition 1 is true if *M(SF) > 0*. This indicates that compromised nodes have gain unauthorized access of data.
  Condition 2 is true if one-third (1/3) of member nodes become compromised;
  If $M(UC_m) + M(DC_m) > 1/3\ (M(T_m) + M(UC_m) + M(FDC_m) + M(DC_m)$

5. ASSESSMENT OF PERFORMANCE-SECURITY METRICS

The two metrics of interest are *mean time to security failure* and *system response time*. From the given SPN model, these two metrics are calculated as follow;

Mean Time to Security Failure: This metric is obtained as the expected accumulated reward until the system goes to any of the absorbing state.

Service Response Time(R): R per group communication packet over the life time of the system is calculated by accumulating wireless contention delay and transmission delay over MTTSF divided by MTTSF [8]. The equations for wireless contention delay and transmission delay are based on [17].

6. RESULTS AND ANALYSIS

Results are calculated by changing design parameters. The following parameters are taken to derive results;

- Joining rate is 4 times higher than the leaving rate, i.e. $\lambda:\mu$ = 4:1
- m=5, i.e. 5 nodes can take part in voting
- Wireless bandwidth is assumed to be 1 Mbps
- IDS interval varies from 30 seconds to 9600 seconds
- initial number of nodes, N_{init} = 60,
- Compromising rate, λ_c= once per 12 hours
- Data request rate, λ_q= once per 30 minutes
- $p_1 = p_2$= 1% = 0.01
- For voting-based IDS P_{fn} and $P_{fp}$are calculated based on the equation given in section 6.4.2.4
- In calculating R, some default values are taken from [17].

The main objective is to determine optimal settings for the group communication system of robots in terms of optimal double threshold k_1 and k_2 of the proposed batch rekeying protocols [18] and optimal IDS interval that maximize *MTTSF* and at the same instant minimize the system response time (R). Specifically, optimal IDS intervals are identified on the basis of the identified optimal double thresholds $k_1$and k_2. The performance-security metrics are assessed and results are compared based on double threshold batch rekeying protocols and most primitive individual rekeying integrated with IDS.

6.1 Optimal Double Thresholds (k_1 and k_2)

The results are calculated by varying the thresholds k_1 *and* k_2 for *TAUDT-C rekeying* technique [8]. Recall that in the given SPN model, for *TAUDT-C rekeying* technique, rekeying is performed only if (*M(TJ)* + *M(TL)*) reaches k_1 OR ($M(FDC_m)$ + $M(DC_m)$) reaches k_2. In figure 2 it is clearly shown that *MTTSF* is above the other curves when k_1 = 1, which means the system will last for long time. This (k_1 = 1) corresponds to immediate eviction of detected compromised nodes without any delay.

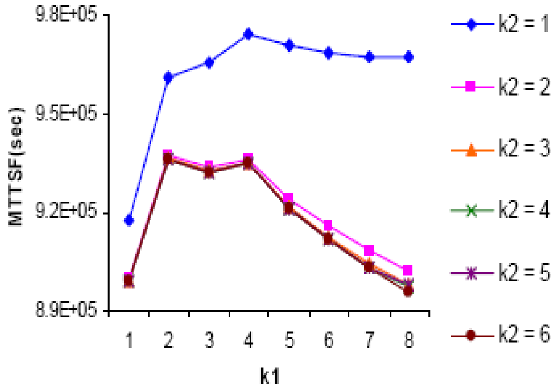

Fig 3: Optimal Double Thresholds (k_1 and k_2) for *TAUDT-C* in *MTTSF*

Under *TAUDT-C rekeying* technique, the optimal *MTTSF* is observed at (k_1,k_2) = (4,1). Now, let us explore why *MTTSF* is optimal at this double threshold? Recall that k_1 is a threshold that is associated with number of join/leave nodes, i.e. *M(TJ)* + *M(TL)*and k_2 is another thresholds that is associated with detected compromised nodes, i.e. $M(FDC_m)$ + $M(DC_m)$. As k_2 is increased, there will be more detected compromised nodes in the system due to which the system may reach security failure state due to condition 1. It is observed that if k_2 becomes greater than 1, the *MTTSF* significantly deteriorates.

As $k_1$is increased, detected compromised nodes will quickly be evicted from the system. This is because the probability that rekeying is performed due to k_2 is also increased with increasing k_1, as a result *MTTSF* also increases as shown in the figure. It is also observed that when k_2 goes greater than 1, *MTTSF* is not much affected as k_2 is a threshold that is associated with untrusted nodes and is directly related to security failure. To this end, it is observed that the optimal double thresholds *(k_1, k_2)=(4, 1)* under TAUDT-C rekeying technique as shown in figure 3.

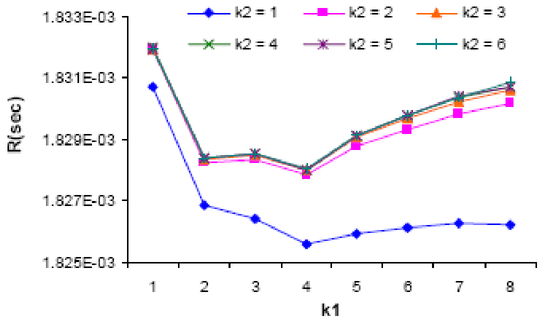

Fig 4: Optimal Double Thresholds (k_1 and k_2) for *TAUDT-C* in *R*

In figure 4, plots of *service response time (R)* are shown. The results are calculated by varying the thresholds k_1 *and* k_2 for TAUDT- C rekeying technique. From the derived results, it is observed that the *R* is also optimized at *(k_1, k_2) = (4, 1)*, which matches the optimal double thresholds in *MTTSF*. Plots for JAUDT- C rekeying protocol are not shown here but it is found that the optimal thresholds for *JAUDT- C* are at *(k_1, k_2) = (5, 2)* both for *MTTSF* and *R*.

As depicted in the results, the design goal is achieved by choosing an optimal threshold for triggering rekeying. The results show that *MTTSF* is maximized while satisfying performance requirements in terms of *R*.

6.2 Optimal Intrusion Detection Intervals

In this section optimal intrusion detection interval *(T_{IDS})* is identified on the basis of the optimal double thresholds k_1 and k_2, which are *(k_1, k_2) = (4, 1)* for TAUDT- C rekeying technique and *(k_1, k_2) = (5, 2)* for JAUDT- C rekeying technique as shown in the previous section. In figure 5, results are shown for *MTTSF* under periodic batch rekeying techniques and the individual rekeying technique (the most primitive one). It is observed that for optimal double thresholds k_1 and k_2, periodic batch rekeying technique outperforms individual rekeying technique in the presence of IDS.

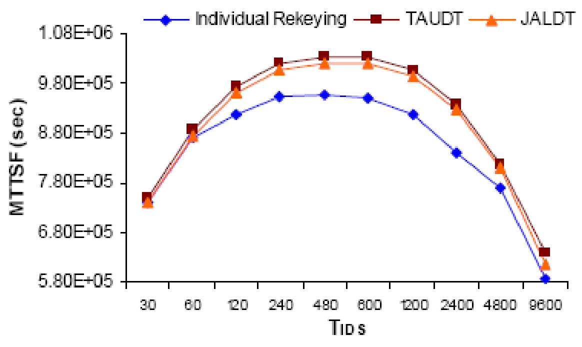

Fig 5: Optimal T_{IDS} in *MTTSF*

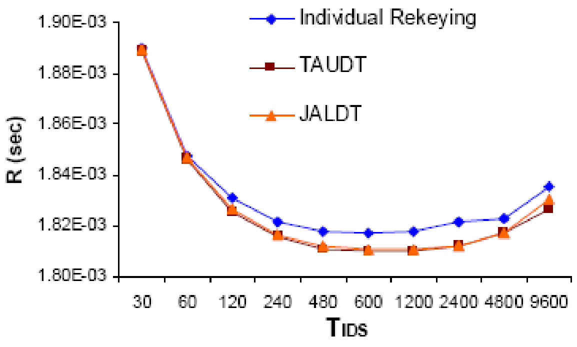

Fig 6: Optimal T_{IDS} in *R*

It is observed from the results that *MTTSF* maximizes at optimal intrusion detection interval. Generally, *MTTSF* go on increasing with the increase in T_{IDS} until the optimal T_{IDS}, after the optimal T_{IDS}, the *MTTSF* go on decreasing as shown in figure 5. The results reveal that performance of the *individual rekeying* technique is the worst as expected and *TAUDT- C* performs the best in terms of *MTTSF*. The optimal intrusion detection for *individual rekeying* is T_{IDS} = 240 seconds, for *TAUDT- C* and *JALDT - C rekeying*, optimal T_{IDS} = 480 seconds as shown in figure 5.

In figure 6, plots of *R* versus T_{IDS} are provided. It is again identified that *R* minimizes at an optimal IDS interval. The same reasoning (as for *MTTSF*) applies for *R* as well. *Individual rekeying* has the worst performance whereas *TAUDT - C* performs the best at the optimal IDS interval. These results can be used by system designers to select T_{IDS}, such that under which system performance is optimized. From figure 5 and 6, it is identified that *MTTSF* is maximize at T_{IDS} = 480 seconds, and *R is minimize* at T_{IDS} = 600 seconds. The results show that optimal T_{IDS} = 480 seconds, under which *MTTSF* is maximized and *R* is minimized, and thus achieving the design goal.

7. CONCLUSIONS

A detailed review and interpretation of the SPN model proposed be Cho et al [8], is performed. Mathematical results are interpreted in more detail to study the performance-security trade-off in the context of RANETs. It is identified that the performance-security trade-off in MANETs, and thus RANETs can be investigated by choosing *MTTSF* as security metric and, *service response time (R)* per group communication packet, as performance metric. A maximum *MTTSF* and minimum *R* at the same instant are desired in RANETs. Optimal results can be obtained by choosing an optimal eviction threshold and optimal IDS interval for rekeying.

8. ACKNOWLEDGMENTS

Firstly, thanks to almighty Allah, the most merciful and the most beneficent, for giving us strength and ability to accomplish this work. Secondly, thanks to our families for their prays and for providing us their unequivocal support throughout, as always. Finally, thanks to Prof. Demtres D. Kouvatsos (SCIM, University of Bradford, UK) for his continuous guidance, assistance and inspiration.

9. REFERENCES

[1] Wolter, K., Reinecke, P. (2010) Performance and security trade-off. In Aldini, A. (Ed.), Proceedings of SFM 2010, LNCS 6154, 135-167. .

[2] S. K. Sarkar, T. G. Basavararaju and C. Puttamadappa "Ad hoc Mobile Wireless Networks Principles, Protocols and Applications". Auerbach Publications 2008.

[3] Kouvatsos, D. D. and Miskeen, G. M., "Performance Related Security Modelling and Evaluation of RANETs", springer, 2012

[4] Asokan, A., Natarajan, A.M., "Quality of Service (QoS) Routing in Mobile Ad Hoc Networks." IGI global, 2010.

[5] Das, S. M., Hu, Y. C., George, C. S., & Lu, L. Y. (2007). Mobility-aware ad hoc routing protocols for networking mobile robot teams. Journal of Communications and Networks, 9(3), 296-311.

[6] Robinson, K. P. (2008). Cooperation using a robotic ad hoc network made from Bluetooth, J XTA, OSGi and other commercial off the shelf (COTS) products. Masters by Research Thesis, Queensland University of Technology, Australia.

[7] Ardawi, A. M. H, "Performance Modeling and Evaluation of Robotic Mobile Wireless Ad Hoc Networks.", MSc Thesis, NetPen – Networks and Performance Engineering Research Unit, IRI - Informatics Research Institute, University of Bradford, Bradford, UK (Sept. 2010).

[8] Cho,J.-H., Chen, I.-R. and Feng, P.-G. "Performance analysis of dynamic group communication systems with intrusion detection integrated with batch rekeying in mobilead hoc networks." AINAW '08: Proceedings of the 22nd International Conference on Advanced Information Networking and Applications { Workshops, pp. 644{649, Washington, DC, USA, 2008.

[9] Kouvatsos, D. D. (2010). Performance modeling and evaluation of RANETs. PP Presentation at the 1st ETSI Workshop on "Networked Mobile Wireless Robotics", Munich, Germany. http://workshop.etsi.org/2010/201010_NetworkedMobileWirelessRobotics/06%20Kou vatsos%202010-10 08%20Networked%20Robots.pdf

[10] Kouvatsos, D. D., Miskeen, G. M. A. (2011). Networked mobile wireless robotics. Technical Report DDK-NetPEn 15-02-11, Networks and Performance Engineering (NetPEn) Research Group, Informatics Research Institute (IRI), University of Bradford, UK, pp. 1-3.

[11] Brutch, P., and Ko , C., "Challenges in Intrusion Detection for Wireless Ad-hoc Networks," *Proc. Symposium on* Applications and the Internet Workshops, 27-31 Jan. 2003, pp.178 – 373.

[12] Cho, J.H., Chen, I. R., and Eltoweissy, M., "On Optimal Batch Rekeying for Secure Group Communications in Wireless Networks," ACM/Springer Wireless Networks, 2007#

[13] Patrick P.C. Lee, John C.S. Lui, and David K.Y. Yau, "Distributed Collaborative Key Agreement and Authentication Protocols for Dynamic Peer Groups," *IEEE/ACM Transactions on Networking*, vol. 14, no. 2, April 2006, pp.263-276.

[14] Li, X., Yang, Y.R., Gouda, M. G. and Lam, S.S. "Batch Rekeying for Secure Group Communications," Proc. of the Tenth Int'l Conf. on World Wide Web, Hong Kong, July 2001, pp. 525-534.

[15] Huang, Y. and Lee, W., "A Cooperative Intrusion Detection System for Ad Hoc Networks," *Proc. 1st ACM Workshop on Security of Ad-hoc and Sensor Networks*, Fairfax, Virginia,2003, pp. 135-147.

[16] Patrick P.C. Lee, John C.S. Lui, and David K.Y. Yau, "Distributed Collaborative Key Agreement and Authentication Protocols for Dynamic Peer Groups," *IEEE/ACM Transactions on Networking*, vol. 14, no. 2, April 2006, pp. 263-276.

[17] Bianchi, G., "Performance Analysis of the IEEE 802.11Distributed Coordination Function," IEEE Journal on Selected Areas in Communications, vol. 18, no. 3, Mar. 2000, pp. 535-547.

[18] Gärtner, F. C., "Byzantine Failures and Security: Arbitrary is not (always) Random," *Technical Report IC/2003/20*, EPFL, April, 2003.

[19] Jeffrey W. HerrmannEdward Lin, Petri Nets: Tutorial and Applications, CIM Lab, Institute for Systems Research, University of Maryland, College Park, Maryland INSTITUTE FOR SYSTEMS RESEARCH. *A National Science Foundation Engineering Research Center, supportedby NSF, the University of Maryland, Harvard University, and Industry.*The 32th Annual Symposium of the Washington Operations Research - Management Science Council,Washington, D.C.