Journal of Medical Systems (2019) 43: 115
https://doi.org/10.1007/s10916-019-1231-7

MOBILE & WIRELESS HEALTH

Adaptive Risk Prediction and Anonymous Secured Communication in MANET for Medical Informatics

Naveena Ambidi[1] · Rama Linga Reddy Katta[1]

Received: 26 December 2018 / Accepted: 27 February 2019 / Published online: 23 March 2019

Abstract

Location-based services (LBS) and information security is a major concern in communication system.With the increasing popularity of location based services more attention is paid to preserve location information to protect the data. In order to protect and preserve the MANET and location based services, there are various existing location based anonymity protocols such as k-anonymity location based, but these protocols are more overhead due to the dynamic mobility nature of ad-hoc networks. In this paper we proposed an Adaptive Risk Prediction and Anonymous Secured Communication protocol to predict the risk before processing anonymous communication. The proposed protocol estimates the risk against adjacent nodes and estimates the vulnerability paths using hidden markov model and decision tree. The decision tree determines the evidence to identify the trusted paths. The anonymous communication message authentication scheme assigns the anonymous communication and organize the secured authentication scheme. We simulated the network by considering different attacks to determine the efficiency of Adaptive Risk Prediction and Anonymous Secured Communication using NS2 simulator.

Keywords MANET · HMM · Decision tree · Risk estimation

Introduction

Mobile nodes in case of MANETs are very useful in application areas like disaster management, emergency and rescue operations that forms a self – organized infrastructure and provides flexibility. However, inherent vulnerability in such network increases the risk of security. Though, MANETs are dynamic and cooperative in nature, economical and effective security mechanisms are needed to safeguard the mobile nodes.

In typical MANET environment, mobile nodes need to protect itself, to prevent against unknown users or nodes. Nodes adopt anonymity approach to protect the actual information. But due to the mobility, the node needs to update the anonymity information for every cyclic period. However estimating a risk can save some amount of anonymity process. To determine a risk, we need to estimate risk level, whenever the mobile nodes interacts within the communication range. However the adopted anonymity process in a communication system may not ensure the node complete trust, this could be an interesting fact to justify the anonymity efficiency.

Wireless Medical healthcare application offers a number of challenges, like, reliable transmission of data, secured data transmission, nodes mobility, detection of event delivery of data in time, power management, etc. Deploying new technologies in healthcare applications without considering security often makes patient privacy vulnerable. For instance, the patient's physiological vital signals are very sensitive so the leakage of the patient's diseased data is not acceptable. Further, wireless medical sensor networks cover a broad range of healthcare applications, such as physiological data monitoring, activity monitoring in healthclubs, location tracking for athlete are the broad range of healthcare applications. WMSNs share individual data with physicians and insurance companies. Thus unauthorized collection and use of patient data by adversaries can cause life-threatening risks to the patient and make the patient's private matters publically available.

Neighbor node anonymity means that each node does not know the real IDs of its neighbor nodes [1]. Let each node communicate anonymously with neighbor nodes. Specifically, whenever a node disconnects with a neighbor node, it randomly

This article is part of the Topical Collection on *Mobile & Wireless Health*

✉ Naveena Ambidi
aambidinaveena@gmail.com

[1] G. Narayanamma Institute of Technology and Science, Hyderabad, India

changes its pseudonyms in all communication layers (e.g., MAC address, IP address) and communication parameters (e.g., signal strength), which will be used for the communication with the next encountered node. Note that both MAC and IP addresses can be easily modified through software [1, 2].

The main idea of this research is to classify the vulnerability to determine the risk level in MANET. In anonymous communication system, nodes need to maintain the anonymity for certain time being, during the mobility process where each nodes interacts with known and unknown nodes. To organize privacy, each node maintains the node anonymity to safeguard against attacks. To prevent such kind of causes, a risk prediction and risk estimation is an important aspect to design efficient anonymous system to observe the fake users or nodes and predict forgery for large scale network for frequent communication causes. Here the classification of vulnerability is based on the node [3, 4].

In this paper, our goal is to protect a node anonymity by estimation and prediction of risk against unknown users. We contributed these steps to achieve efficient and scalable anonymity system.

1) A mobile node can deploy a risk estimator model to communicate with any node without sharing of actual location information
2) A risk predictor and estimator minimize the anonymity errors or learning rate by modeling a network
3) Estimate the vulnerability path to determine the trusted paths
4) Design an anonymous secured message authentication scheme to organize efficient anonymous and secured communication. The rest of the paper is as follows: Section 2,3 deals with related work and attack model. Section 4,5 deals with the proposed technique ARPASC and the anonymous secured communications. Simulation results and discussions are dealt in Section 6. Conclusions are presented in Section 7.

Related work

The routing attacks cause the most devasting damage to MANET. Isolating routing attacks produce more uncertainty to the network. To mitigate such routing attacks and predicting a risk against such routing attacks in Manet, Ziming Zhao et.al [5] proposed risk-aware approach extending the Dempster-Shafer mathematical theory to derive the risk evidence. Ping Zhao et al. [6], proposed *k*-Anonymity based Privacy Preserving against Location Injection Attacks. Jie cui et.al [7] proposed a novel location privacy preserving scheme, in which the vehicles generate a dynamic virtual locations based on the surrounding circumstances. In [8], the authors deals with location anonymity and privacy by proposing an efficient and secure anonymous communication for location based service using asymmetric cryptography to preserve and organize secured communication using asymmetric cryptography scheme. This scheme ensures only the user privacy, but they didn't clearly disclosed about location anonymity.

T. Sarathamani, and Dr. M. Rajesh Babu [9], discussed about anonymity routing problem in MANET by improving the hiding of nodes identity problem, with the deployment of anonymity method, which is known as Robustand Secure Anonymity Protection (RSAP).

Hui Xia et.al [10], proposed a novel light-weight subjective trust inference framework, which organizes trust in two different phases, trust assessment and trust prediction.

In Manets, risk mitigation is possible by vulnerability analysis. Not much research has been done on vulnerability assessment and information security risk management in MANETs because of the mobility of the nodes and lack of a clear line of defense,Cai et al. [11]. Researchers have primarily focused on either evaluating trust of communication between the nodes for vulnerability analysis, Liu et al. [12]; Dai et al. [13], or intrusion detection, Zhang et al. [14]; Bhargava et al. [15]; Mishra et al. [16].

Most of the studies related to vulnerability assessment in MANETs focus on analyzing their risk considering the trust or credibility of each node. The hop distance between adjacent nodes, Takagi et al. [17] and the relative angle of the path are taken into consideration by most routing algorithms to address the mobility of the network (Cao et al. [18]; Giruka et al. [19]. The existing route discovery methods ignore the inherent vulnerability of the nodes for routing decisions, and a comprehensive information security risk assessment model is lacking for emergency.

Now, there are many threat identification methods [20], vulnerability identification methods [21] and asset identification methods [22]. These methods provide the basic data for risk assessment. But how these data must be integrated is a very important task. Shen et al. [23] puts forward the Markov game theoretic data fusion approach for this.

Alvaro et al. [24], implemented intrusion detection in Manets, using Hidden Markov Model Sequential Hypothesise Tests. Maryam Miri Estahbanati et al. [25], used Markov chain trust based routing. Saini Das et al. [26], in their work proposed a Markov based model for Information Security Risk Assessment in healthcare MANETs. Anusha Kannan et al. [27], proposed a decision tree based rule formation with a combination of PSO-GA algorithm for intrusion detection system.

It can be observed in the literature that many works were developed for risk assessment in Manets based on trust computations [30]. Few works were developed for risk assessment using techniques like Markov models but could not provide complete Anonymity. This paper attempts to fulfill these gaps by proposing an efficient Markov-based information security risk prediction model in Anonymous Manet environment.

Attack model

The attacks are categorized based on the attack behavior, the most common attack models are, active attacks and passive attacks [28]. The active attacks prevents a networks flow between pair of nodes <*S* : *D*>, it has two different attack natures such as internal attacks and external attacks. The internal attacks attack inside a network which mainly targets on source and adjacent nodes, which are more vulnerable compare to the external attack. The external attack carried out the attack process outside of the network, without considering a specific node, it can take control on communication channels. The passive attacks doesn't alter the data communication, but it listen to the communication to interrupt the communication services.

In this research work, we considered following attack assumptions,

1) The probability of active attack on over anonymous communication
2) The probability of anonymous node compromization due to the lack of risk estimation
3) The probability of path failure due to the untrusty adjacent nodes

Adaptive risk prediction and anonymous secured communication (ARPASC)

Overview

The main purpose of proposed model is to identify and predict the risk on the basis of anonymity and MANET nature. Now as an extension to the previous work, we propose to design an adaptive risk prediction and anonymous routing protocol to predict the attack probability in MANET using hidden markov model and decision tree approach [6, 7]. The proposed protocol organizes the anonymous prediction and detection approach in risk estimation, path vulnerability estimation and evidence collection, and the anonymous communication is represented in anonymity hop sequence generation, anonymous secured message authentication. The detailed process is described in below sections to determine the protocol efficiency for various malicious nodes.

Risk estimation

The risk estimation function determines $f(r_i)$, the risk against its corresponding neighbours. A risk estimation considers each node anonymity history attribute. The ratio of node interactivity with other anonymous node. Initially the source node broadcasts the beacon message. The neighbouring nodes receive the beacon messages. Association stability is calculated based on the number of beacons recorded which is updated in risk estimation probability function [8, 9].

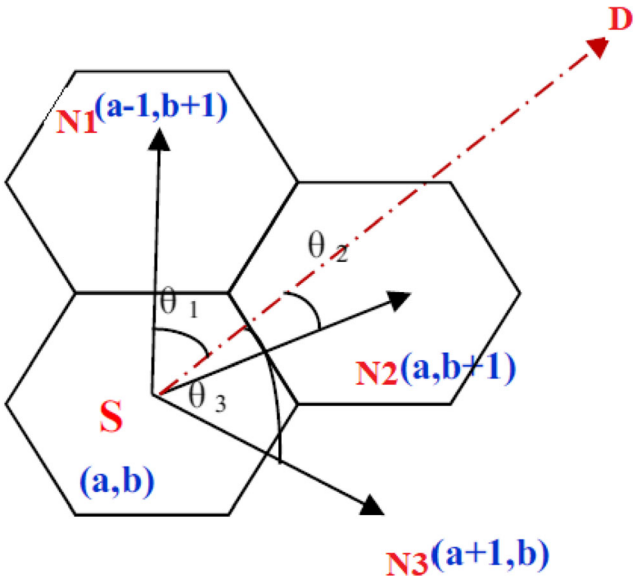

Fig. 1 Angle risk estimation

$$Risk\ Estimation\ probablity = f(a, d, M, ct) \quad (1)$$

Where a = Angle, d = Distance, M = Mobility, ct = Compromise Time.

Let consider a set of source and destination pairs $\{(S_1, D_1), (S_2, D_2), \ldots . (S_{n-1}, D_{n-1})\}$ and a distance across each pair of nodes are $\{d_1, d_2, \ldots, d_{n-1}\}$. When a pair of nodes have random mobility at different time instances, the risk probability of each node with corresponding destination and adjacent nodes will be as

$$\sum_{k=1}^{n} P(N_k) = p(a_k)p(d_k)p(M_k)p(ct_k) \quad (2)$$

According to the Fig. 1, the angle probability $p(a_k)$from an anonymous node to its adjacent anonymous neighbor depends on the angle (i.e., θ1, θ2 and θ3) that each of the three adjacent nodes (i.e., N1, N2 and N3) make with the line drawn from source to destination.

The attacker uses angle criteria to manipulate source and destination pairs. Attacker consider different angles of node, where the attacker can capture the source transition signals. The probabilities of 360-degree angle of a node are measured. The angle probability $p(a_k)$ of moving from node S to one of

Table 1 Risk estimation probability rate matrix

Nodes	Angle probability	Distance probability	Mobility probability	Compromise time probability
1	0.3145	0.3554	0.7	0.2482
2	0.3927	0.3097	0.76	0.3197
3	0.2930	0.3347	0.55	0.432

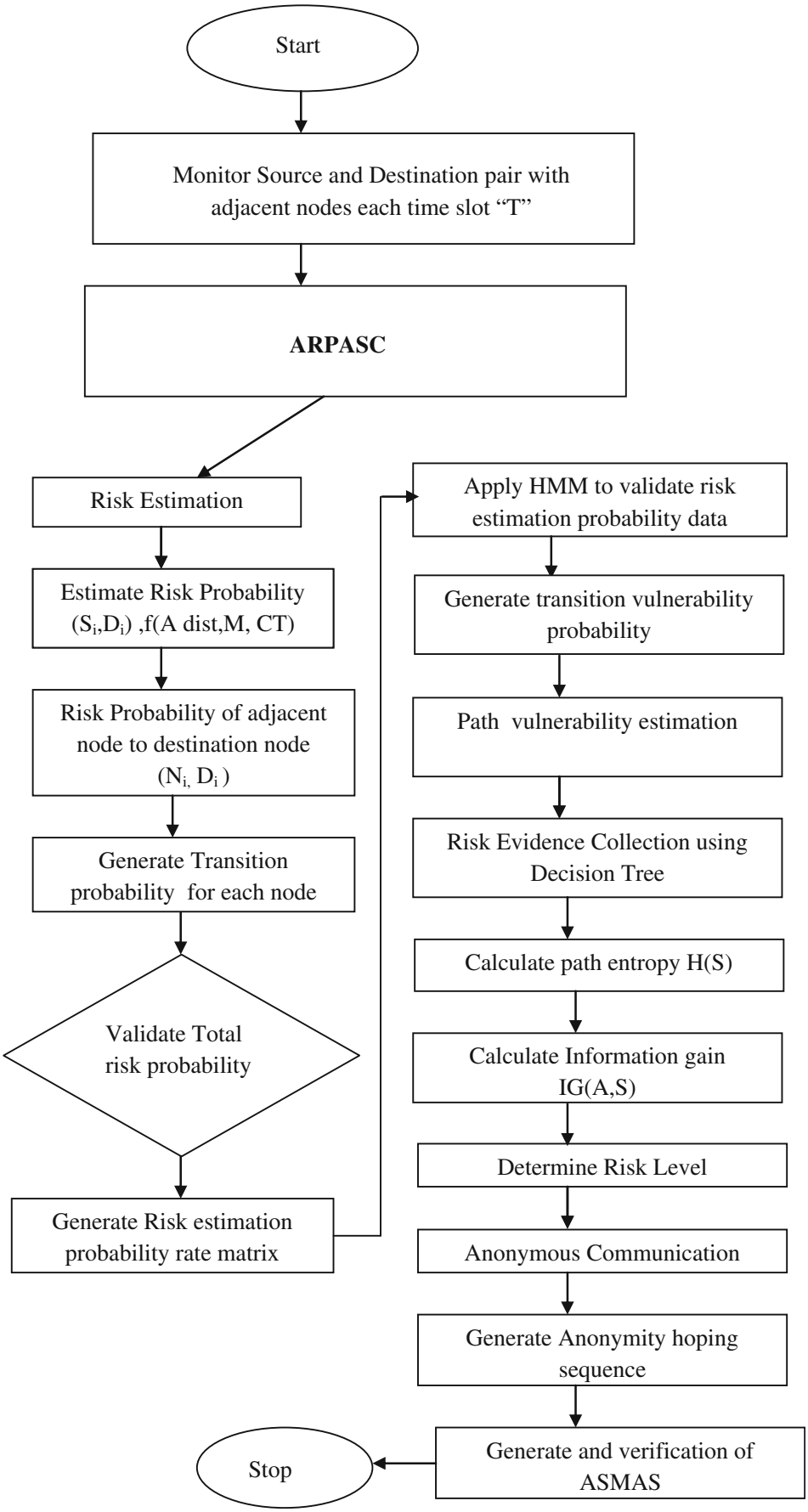

Fig. 2 Flow diagram of proposed ARPASC technique

Table 2 Simulation parameters

No. of nodes	200
Area size	1000 × 1000
Mac	IEEE 802.11b
Transmission range	250 m
Simulation time	200 s
Traffic source	CBR
Packet size	512
Mobile speed	10,20,30,40 and 50 m/s
Attackers	5,8,10,12
Initial energy	10 J
Transmission power	0.6 60 J
Receiving power	0.3 95 J
Routing protocol	ARPASC
Antenna	OmniAntenna

the n adjacent nodes is presented in Eq. 2, where, angle N1→ S→N3 = 120°; and 120° ≤ θ1 + θ2 + θ3 ≤ 180°; for $n = 3$.

$$pa_k = 0.5X\left(1-\frac{\theta_k}{\left(\sum_{k=1}^{n}\theta_k\right)}\right) \tag{3}$$

However the distance is also another possibility to the attacker to attack on a source node. The distance probability of a source node S is estimated between the adjacent node ($N1$, $N2$, $N3$) to targeted destination D and is measured with the non orthogonal location coordinates. The Eq. 4 represents the distance measurement.

$$dist_{(i_0,j_0)(i_k,j_k)} = \sqrt{(j_k-j_0)^2+(i_k-i_0)^2+(j_k-j_0)\times(i_k-i_0)} \tag{4}$$

The probability of distance is shown in Eq. 5:

$$pd_k = \frac{dist_k}{\left(\sum_{k=1}^{n} dist_k\right)} \tag{5}$$

where $dist_k = \log_{10} dist_{(i_0,j_0)(i_k,j_k)}$,where $n = 3$.

Compromised time (ct) is used to determine the time taken probability to attack on the nodes. The attacker keenly observes the sources, and its adjacent nodes (i.e N1,N2,N3). The compromised time attack probability for n adjacent nodes is defined in Eq. 6, which it considers the total time elapsed (t) and vulnerability severity (vs).

$$pct_k = \frac{1-ct_k}{\left(\sum_{k=1}^{n} ct_k\right)}, \tag{6}$$

where $n = 3$ and $ct_k = \sum_{i=1}^{n} \frac{1}{t_i vs_i}$ where the i = {1 to n},

n is number of vulnerabilities.

Generally attacker randomly moves to the different corners of the network to compromise the sources and its adjacent nodes, to move across the network, the attacker selects the different sources and adjacent nodes angles θ. Based on the distance rate and angle rate, the attacker organizes the velocity rate, to determine the mobility probability. The attacker takes consideration of adjacent nodes mobility rate i.e. velocity v.The attacker estimates the mobility probability rate of adjacent nodes from source node which is measured in Eq. 7.

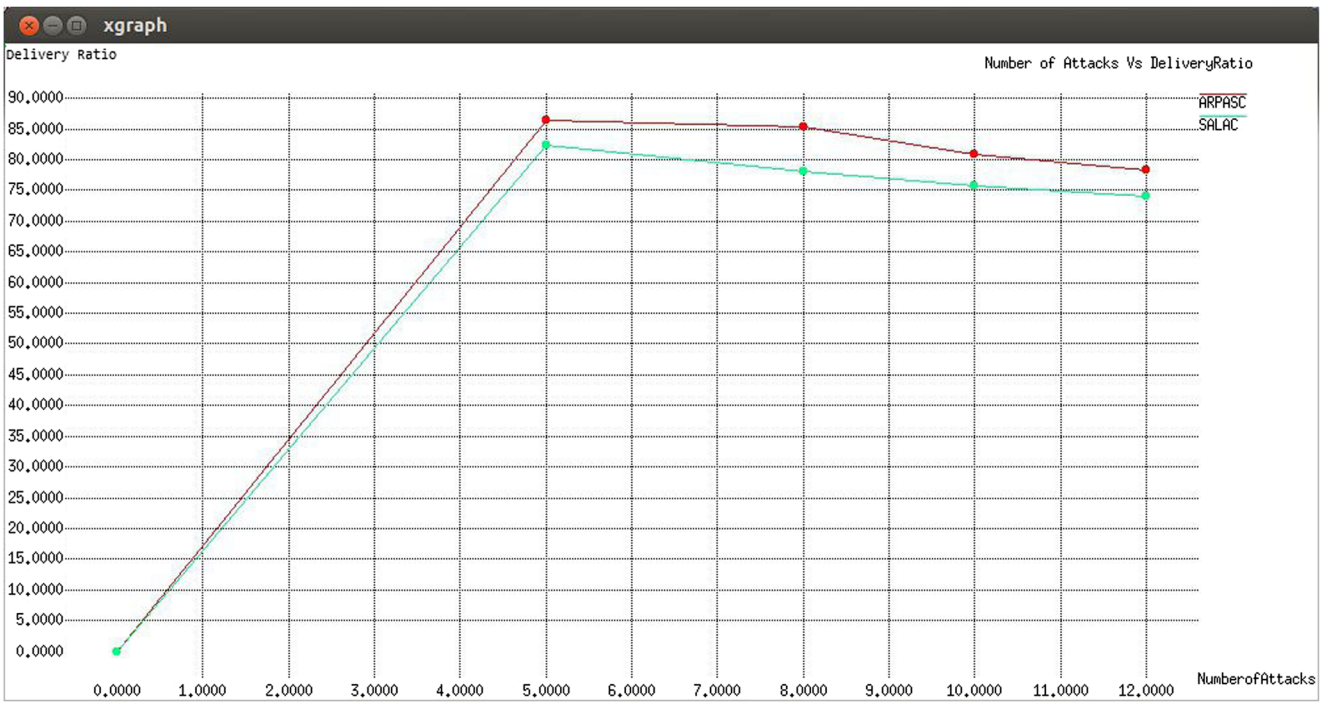

Fig. 3 Number of attackers vs packet delivery ratio

Input: Set of states s, time t
Output: Estimate minimum and maximum number of hops to attack

1) Initialize set of states $s = \{s_1, s_2, \ldots, s_i\}$ where $s_i = \{pa_k, pd_k, pM_k, pct_k\}$

2) Begin process moves from s_{ik-1} one state to another s_{ik} generating a sequence of states $s_{i1}, s_{i2}, \ldots, s_{ik}$:

3) probability of each subsequent state

$$P(s_{ik}|s_{i1}, s_{i2}, \ldots, s_{ik-1}) = P(s_{ik}|s_{ik-1})P(s_{i1}, s_{i2}, \ldots, s_{ik}) = P(s_{ik}|s_{i1}, s_{i2}, \ldots, s_{ik-1})P(s_{i1}, s_{i2}, \ldots, s_{ik-1}) = P(s_{ik}|s_{ik-1})P(s_{i1}, s_{i2}, \ldots, s_{ik-1}) = \cdots$$

$$= P(s_{ik}|s_{ik-1})P(s_{ik-1}|s_{ik-2}) \ldots P(s_{i2}|s_{i1})P(s_{i1}) \quad (9)$$

4) Generate random observation states $\{v_1, v_2, \ldots, v_M\}$ i.e where states are not visible

5) Compute Risk estimation Transition probability

5.1 matrix of transition probabilities $REP_{ij} = P(s_i|s_j)$

$$P(\{pa_k, pd_k, pm_k, pct_k\}) = P\left(\frac{pa_k}{pd_k}\right)P\left(\frac{pd_k}{pm_k}\right)P\left(\frac{pct_k}{pd_k}\right) \quad (10)$$

5.2 matrix of observation probabilities $B = (b_i(v_m)), b_i(v_m) = P(v_m \mid s_i)$

5.3 vector of initial probabilities $\pi = (\pi_i)$, $\pi_i = P(s_{ik})$ and initial probability

6) Represent model $M = (REP, B, \pi)$.

7) Find minimum and maximum number of hops

$$H_{min} = \frac{P_{ik}^{n}}{P_n(S:D)} > 0 \;\&\&\; \frac{P_{ik}^{n-1}}{P_n(S:D)} < 1 \quad (11)$$

$$H_{max} = \frac{P_{ik}^{n}}{P_n(S:D)} = 1 \;\&\&\; \frac{P_{ik}^{n-1}}{P_n(S:D)} < 1 \quad (12)$$

8) Derive the minimum number of hops to reach from source to destination $< S:D >$ at n^{th} step is $P_n(S:D)$

9) The overall transition vulnerability probability is

$$P(VE) = (H_{min}, H_{max}, REP, B, \pi) \quad (13)$$

$$pM_k = 1 - \frac{M_k}{\left(\sum_{k=1}^{n} M_k\right)} \quad (7)$$

where $M_k = rand(v)$ Where the $n = 3$, where v is velocity which represent the node mobility speed.

Based on all the probability rates which were defined in Eqs. (4) (5) (6) (7), the total risk probability based on different time instances are measured by assigning different weights to the each criteria. Let assume W_1, W_2, W_3, W_4 are four different weights, we consider each weight as 0.25. The total risk probability based on the four-criteria probability rate from source to adjacent nodes are derived as $P(REP)$ as in Eq. 8.

$$P(REP) = pa_k \times W_1 + pd_k \times W_2 + pM_k \times W_3 + pct_k \times W_4 \quad (8)$$

If the total probability rate in between $0.75 \geq P(REP) \leq 1$, will be considered as high vulnerability rate. If $P(REP)$ in between $0.5 \geq P(REP) < 0.75$, will be considered as medium vulnerability rate. If $P(REP)$ rate is less than 0.5 will be treated as less vulnerable.

Based on the four different criteria probability rate, the Table 1 determine the vulnerability status at each node:

$$S(0,0)\ N1(-1,1)\ N2(0,1)\ \ N3(1,0)\ \ D(1,4)$$

Path vulnerability estimation

The vulnerability estimation $P(VE)$ probability determines the vulnerability rate on each path from all possible paths between source S to the target T. The hidden markoval model validate the risk estimation probability data, by considering risk estimation probability rate matrix table in Table 1. The HMM, considers the four different risk estimation criteria as set of states $s = \{pa_k, pd_k, pM_k, pct_k\}$.

Algorithm 1:

The risks of each attack and response should be calculable, because the attack response actions could cause a lot of damages than attacks. Based on the secure and unsecure states, MANET is divided into two states one is secure and second unsecure state. If the node is compromised by malicious node then it is in unsecure state. If the MANET network is secure, does not mean it is fully safe network. The evidence collection is used to determine whether the network is safe or not.

Risk evidence collection

The risk of each adjacent node in between source and destination pair is defined in probability risk estimation matrix and vulnerability path estimation. The risk of each path and risk of each adjacent node should be determined in the evidence collection by employing the data into the decision tree [10]. The evidence collection, collect the probability state information from our risk estimation matrix table to detect the uncertainty during anonymous communication by computing the entropy. The entropy mechanism determines the optimality by considering different categories of risk estimation matrix data.

Let estimate entropy of each path to determine uncertainty by considering risk estimation matrix data.

$$H(S) = \sum_{c \in C} -p(c)\log_2 p(c) \quad (14)$$

Where S represents set of path states

C presents set of classes $\{H_{min}, H_{max}, REP, B, \pi\}$

$p(c)$ represents the proportions of number of elements in a class C

Where the entropy function determines the different entropy rate values of different paths, the lowest entropy rate value set and highest entropy value set will be assigned to information gain for determining the path efficiency

$$IG(A,S) = H(S) - \sum_{t \in T} p(t)H(t) \quad (15)$$

$H(S)$ entropy of set S.

t sub sets which are created from risk path set S.

The higher information gain of path will be considered as a higher trust probability rate. The risk evidence approach considers the different information gain rate values and evaluates the risk with respective of two different evidences types $RE1$, $RE2$.

$RE1$: The possibility of attack occurrence in a chosen path in between source and destination pair. The risk evidence probability is represented as

$$P(RE1) = f(IG(S)) \quad (16)$$

where the $f(IG(S))$ is a probability attack function which is a representation of information gain attribute rate.

If $\min(IG) < P(RE1) \leq \max(IG)$ will be considered as a trustable path.

$P(RE2)$: proves an evidence of path alter by malicious node, where the path alter function $f(P)$ considers the minimum and maximum hop values $\{H_{min}, H_{max}\}$ and different distance rates,

$$P(RE2) = f(P) \quad (17)$$

$$\text{Attack} = \text{P(RE1)} \oplus \text{P(RE2)} \quad (18)$$

Based on the risk estimation function, the risk level is determined the risk threshold in two different risk threshold bands, such as upper threshold band and lower threshold band. The path should be represented in between $<UT : LT>$.

$$P(p_n) = \left[\frac{\text{Risk} - \text{LT}}{\text{UT} - \text{LT}} * n\right] \quad \text{Risk} \in (LT, UT) \quad (19)$$

Anonymity hopping sequence generation

In a network the generated anonymity hopping sequence are assigned to mobile nodes. The generated anonymity hopping sequence contains the cache about earlier hops. When the

network is interpreted with malicious packets, any two hopping sequences should have a maximum Hamming distance so that a malicious/compromised node can be recognized in a network.

Suppose that the network consist of n nodes with $n-m$ malicious nodes, and let the set of available paths be $\{p_1, p_2, p_3, \ldots, p_{n-1}\}$. To design a, n - anonymity hopping sequences for $P_n(S:D)$ is a pseudonym of $\{H_{min}, H_{max}\}$, the anonymity node executes the following steps

Step 1: Generate n random sequences s_j; $1 \le j \le n$, each of length L. For each sequence $sj = \{sj(1), \ldots, sj(L)\}$, we have $Pr[s_j = k] = 1/K$, where k = 1,2, . . .,K.

Step 2: Generate a random location vector $c = \{c(1), \ldots, c(M)\}$ where $Pr[c(i) = k] = 1/K$ $i = 1, \ldots, M$ *and* $k = 1, 2, ., K$.

Step 3: Generate a random slot position vector $v = \{v(1), .., v(M)\}$, *where* $v(i) \in \{1, .., L+M\}$, $v(i) \neq v(j), \forall\, i \neq j$

Step 4: To assign anonymity hopping sequence to each node.

Anonymous communication (AC)

Suppose a source S wishes to transmit a message m anonymously from adjacent node $\{x_n\}$to destination node. Then the AC consider n adjacent nodes anonymity level as $\int = \{A_1, A_2, . . ., A_n, A_t$, where the actual message sender is A_t, for some value t,$1 \le t \le n$.

Let organize secured anonymous communication by considering a large prime number p and α be a primitive element of Z_p^*. Then α is also a generator of Z_p^*. That is $Z_p^* = <\alpha>$. Both p and α are made public and shared by all members in $\int$. Each $A_i \in \int$ has a public key $y_i = \alpha^{x_i} \bmod p$, where x_i is a randomly selected private key from Z_{p-1}^*.

In this scheme, we do not discriminate between the node A_i and its public key y_i. Therefore, we also have $\int = \{y_1 y_2, \ldots \ldots \ldots . . y_n\}$.

Suppose m is a message to be transmitted. The private key of the message sender is x_t, $1 \le t \le n$.

To generate an efficient anonymous secured message authentication scheme (ASMAS) for message m, by following three steps:

Generation of ASMAS

(1) Select a random and pair wise different k_i, l_i for each $1 \le i \le n$, $i \neq t$ and compute $r_i = \alpha^{k_i} \bmod p$, $s_i = \alpha^{l_i} \bmod p$, $q_i = \alpha^{h_i} \bmod p$ where $1 \le k_i, l_i, q_i < p$.

(2) Choose two integers k, l *randomly where* $1 \le k, l < p$ and compute $r_t = \alpha^k \prod_{i \neq t} y_i^{-r_i} \bmod p$, $s_t = \alpha^l \prod_{i \neq t} r_i^{-s_i} \bmod p$ *and* $q_t = \alpha^h \prod_{i \neq t} s_i^{-q_i} \bmod p$ such that $r_t \neq 1$, $s_t \neq 1$, $q_t \neq 1$, $r_i \neq r_t$, $s_i \neq s_t$, $q_i \neq q_t$ *for each* $i \neq t$.

(3) Compute

$$w = k + l + h + \sum_{i \neq t} k_i + \sum_{i \neq t} l_i + \sum_{i \neq t} h_i + x_t r_t + k_t s_t + l_t q_t \bmod p \quad (20)$$

The ASMAS of the message m is defined as

$$\int(m) = \left(m, \int, r_1 \ldots . r_n, \; s_1 \ldots . s_n, q_1 \ldots . q_n, h_1 \ldots . h_n, w\right) \quad (21)$$

where

$$\alpha^w = r_1 \ldots . r_n s_1 \ldots . s_n q_1 \ldots q_n y_i^{r_1} \ldots y_n^{r_n} \ldots r_1^{s_1} r_n^{s_n} \ldots s_1^{q_1} \ldots s_n^{q_n} \bmod p \quad (22)$$

Verification of ASMAS

A verifier can verify an alleged ASMAS $(m, \int, r_1 \; .. \; .. \; .r_n, s_1 \ldots . s_n, w)$ for message m by verifying whether the following equation

$$\alpha^w = r_1 \ldots . r_n s_1 \ldots . s_n q_1 \ldots . q_n y_i^{r_1} \ldots . y_n^{r_n} r_1^{s_1} \ldots . r_n^{s_n} \ldots . s_1^{q_1} \ldots . s_n^{q_n} \bmod p \quad (23)$$

holds. If (23) holds true, the verifier accepts the ASMAS as valid for message m. Otherwise the verifier rejects the ASMAS. If the ASMAS is validated without being modified, the future anonymous communication is designed as follows

$$\begin{aligned}
&\prod_{i=1}^{n} r_i \prod_{i=1}^{n} s_i \prod_{i=1}^{n} q_i \prod_{i=1}^{n} y_i^{r_i} \prod_{i=1}^{n} r_i^{s_i} \prod_{i=1}^{n} s_i^{q_i} \bmod p \\
&= \left(\prod_{i \neq t}^{n} r_i\right) r_t \left(\prod_{i \neq t}^{n} s_i\right) s_t \left(\prod_{i \neq t}^{n} q_i\right) q_t \left(\prod_{i \neq t}^{n} y_i^{r_i}\right) y_t^{r_t} \\
&\left(\prod_{i \neq t}^{n} r_i^{s_i}\right) r_t^{s_t} \left(\prod_{i \neq t}^{n} s_i^{q_i}\right) s_t^{q_t} \bmod p \\
&= \alpha^{\sum_{i \neq t} k_i} \alpha^{\sum_{i \neq t} l_i} \alpha^{\sum_{i \neq t} h_i} \left(\alpha^k \prod_{i \neq t} y_i^{-r_i}\right) \left(\prod_{i \neq t} y_i^{r_i}\right) y_t^{r_t} \\
&\left(\alpha^l \prod_{i \neq t} r_i^{-s_i}\right) \left(\prod_{i \neq t} r_i^{s_i}\right) r_t^{s_t} \left(\alpha^h \prod_{i \neq t} s_i^{-q_i}\right) \left(\prod_{i \neq t} s_i^{q_i}\right) s_t^{q_t} \bmod p \\
&= \alpha^{\sum_{i \neq t} k_i} \alpha^{\sum_{i \neq t} l_i} \alpha^{\sum_{i \neq t} h_i} \alpha^k y_t^{r_t} \alpha^l r_t^{s_t} \alpha^h s_t^{q_t} \bmod p \\
&= \alpha^{\sum_{i \neq t} k_i + \sum_{i \neq t} l_i + \sum_{i \neq t} h_i + k + l + h} y_t^{r_t} r_t^{s_t} s_t^{q_t} \bmod p \\
&= \alpha^{\sum_{i \neq t} k_i + \sum_{i \neq t} l_i + \sum_{i \neq t} h_i + k + l + h} \alpha^{x_t r_t} \alpha^{k_t s_t} \alpha^{l_t q_t} \bmod p \\
&= \alpha^{k + l + h + \sum_{i \neq t} k_i + \sum_{i \neq t} l_i + \sum_{i \neq t} h_i + x_t r_t + k_t s_t + l_t q_t} \bmod p \\
&= \alpha^w \bmod p
\end{aligned} \quad (24)$$

Then, the destination accepts the message after validating ASMAS message of destination adjacent node. The entire process is shown in flow diagram in Fig. 2.

Simulation results

Simulation model and parameters

In this research work, we simulate a MANET network model with a set of malicious nodes. In order to evaluate the ARPASC

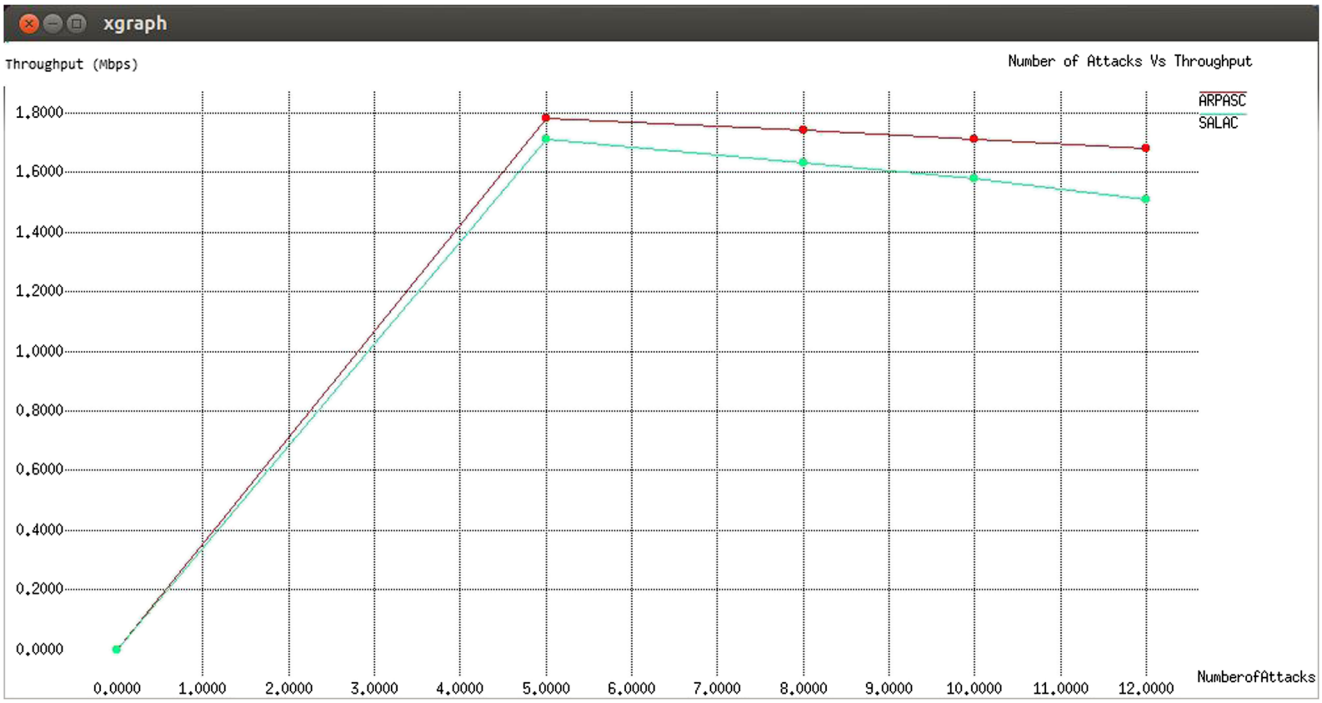

Fig. 4 Number of attackers vs average throughput

efficiency we consider a network with group of active attacks. Each attack configured with set of mobile nodes, with different communication range and energy rate. The attacks are configured with high frequency communication range with high amount of data rate. The Network Simulator (NS2) [29], is used to simulate the network, with different attacking assumptions. In this simulation, we consider a network range as 50 mobile nodes to 200 mobile nodes with the 2 Mbps data rate and with random mobility. We consider a minimum $n/10$ attacking nodes in a network. In this experiment we considered blackhole attack, jamming attack, wormhole attacks and flooding attacks.

In this experiment we modify DSR routing protocol with hidden markoval model and decision tree model. DSR protocol packet is modified with respect to anonymity packet features.

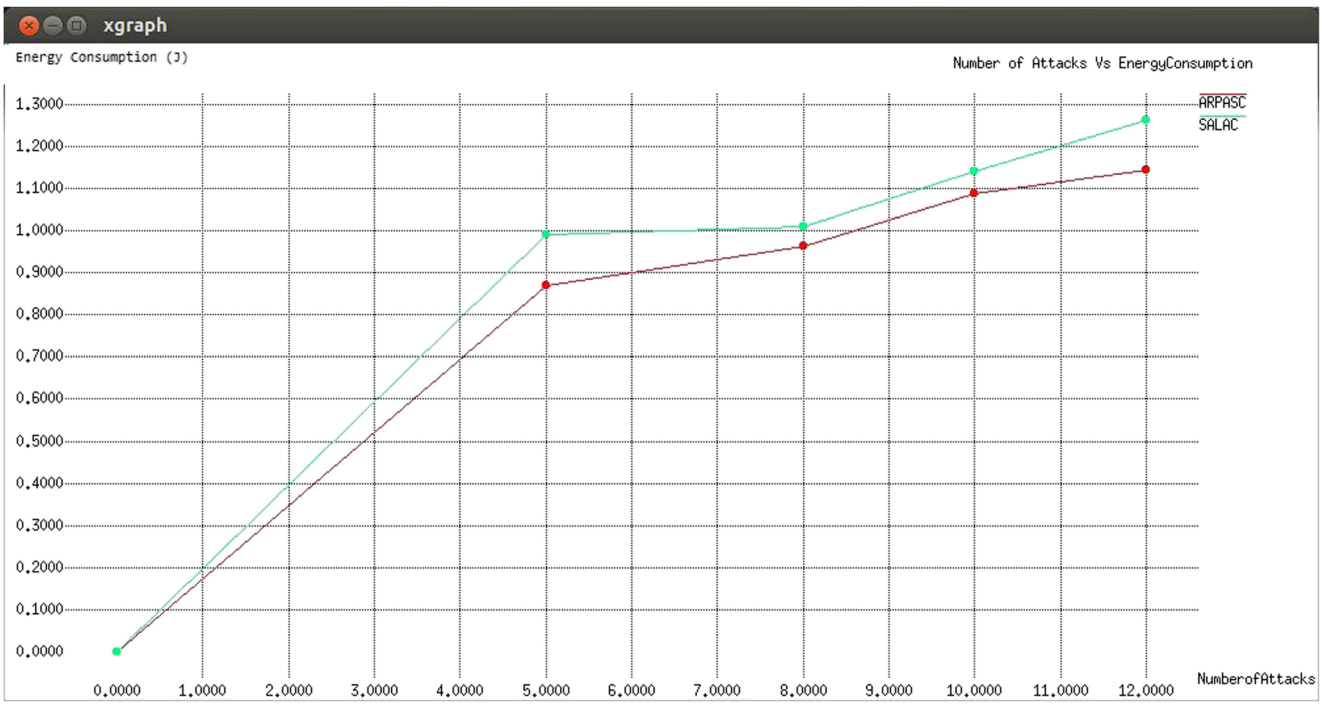

Fig. 5 Number of attackers vs energy consumption

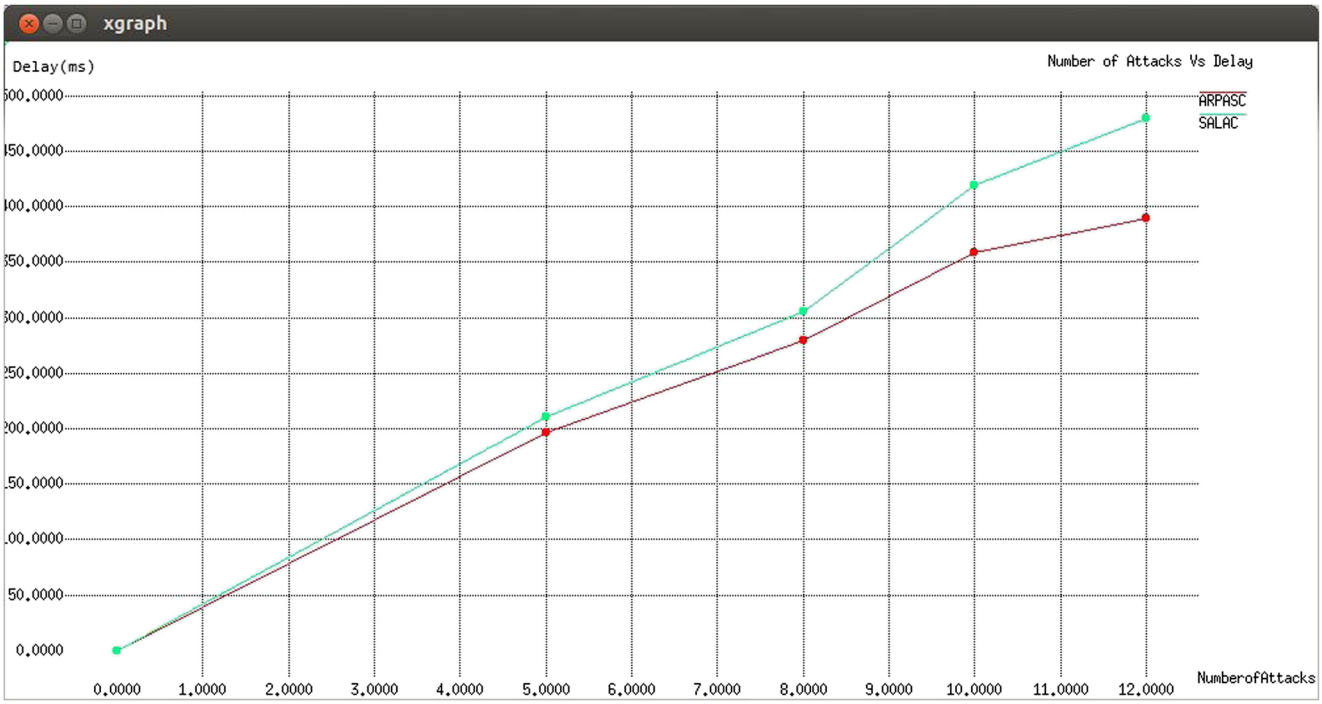

Fig. 6 Number of attackers vs end-to-end delay

The simulation settings and parameters are summarized in Table 2.

Performance metrics

The proposed Adaptive Risk Prediction and Anonymous Secured Communication (ARPASC) is compared with the Secured anonymous communication for location based service using asymmetric cryptography scheme (SALAC) [8]. The performance is evaluated mainly, according to the following metrics.

- **Packet Delivery Ratio:** The ratio of total amount of packets received by total number of packets sent.

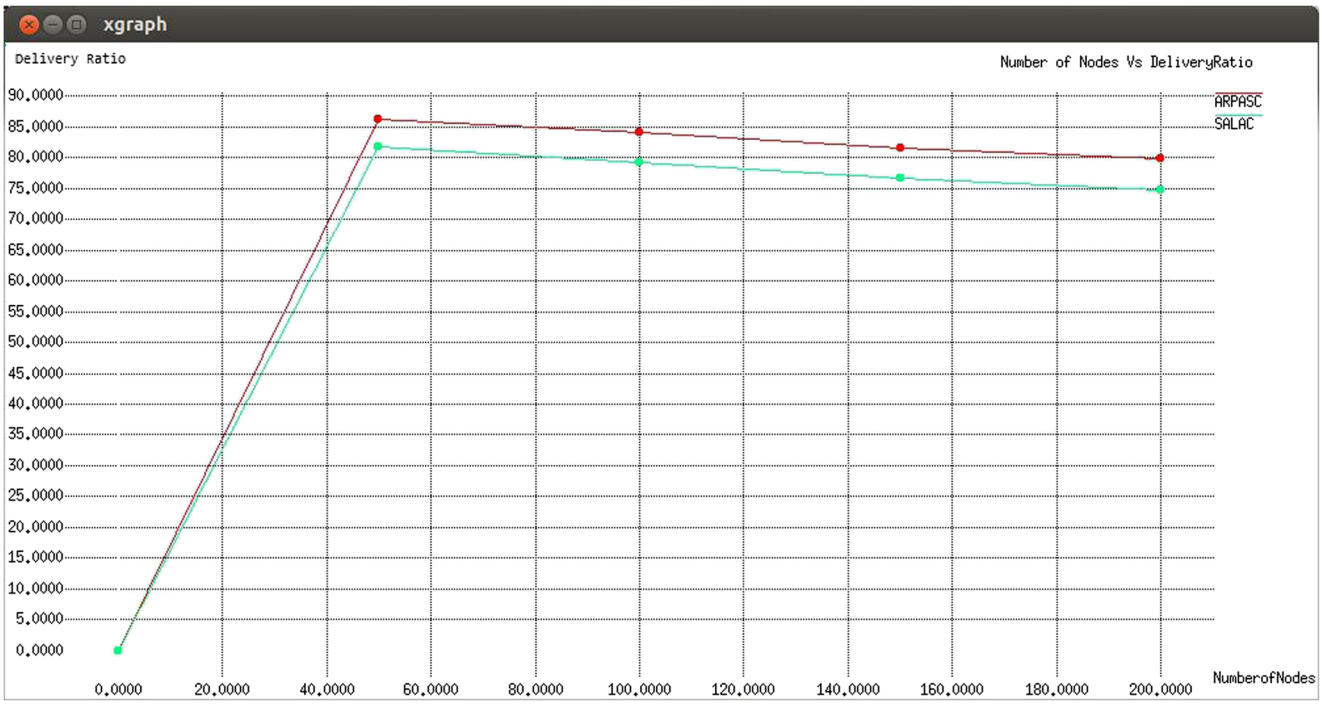

Fig. 7 Number of nodes vs packet delivery ratio

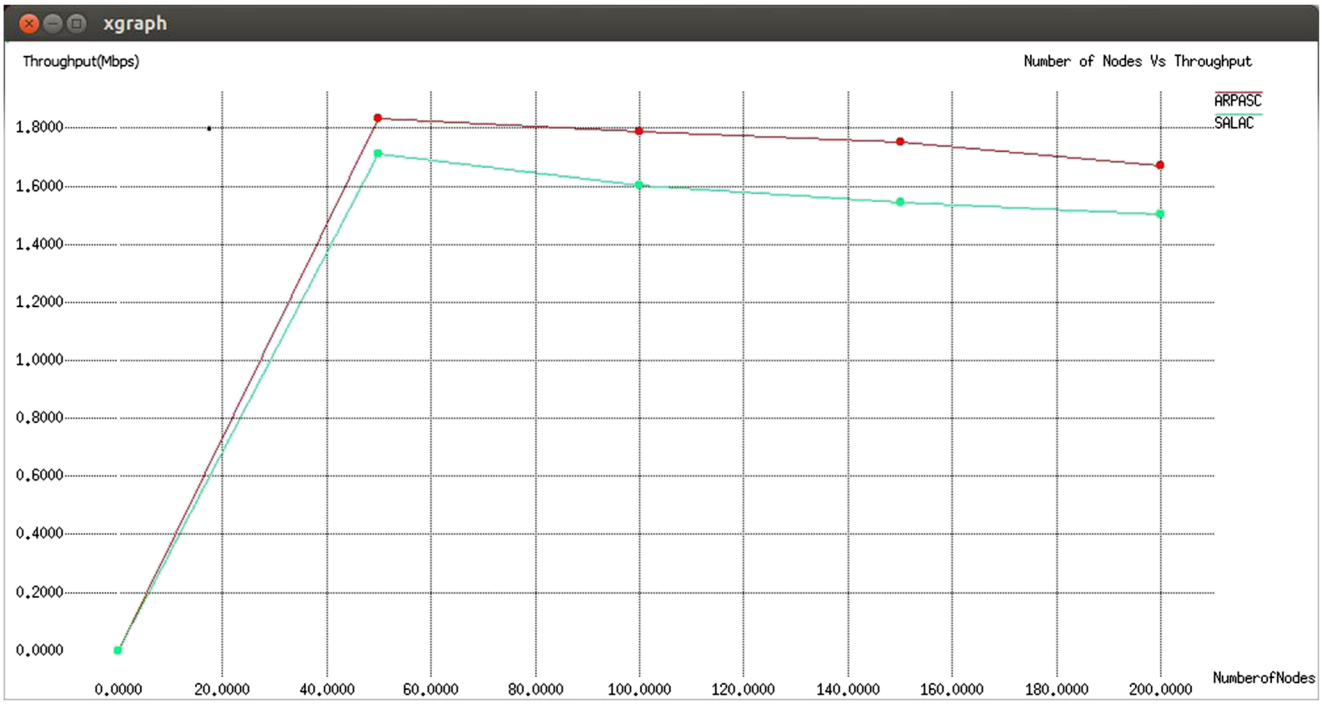

Fig. 8 Number of nodes vs average throughput

- **End to end delay**: The amount of end to end delay during the transmission
- **Energy Consumption**: The total amount of energy consumed by the nodes to transmit the data packets to the receiver.
- **Throughput**: The total amount of data transmitted at destination through the link.

Results

Based on number of attackers

In this scenario we considered blackhole, wormhole and flooding attacks. We have considered minimum 5 attacks.

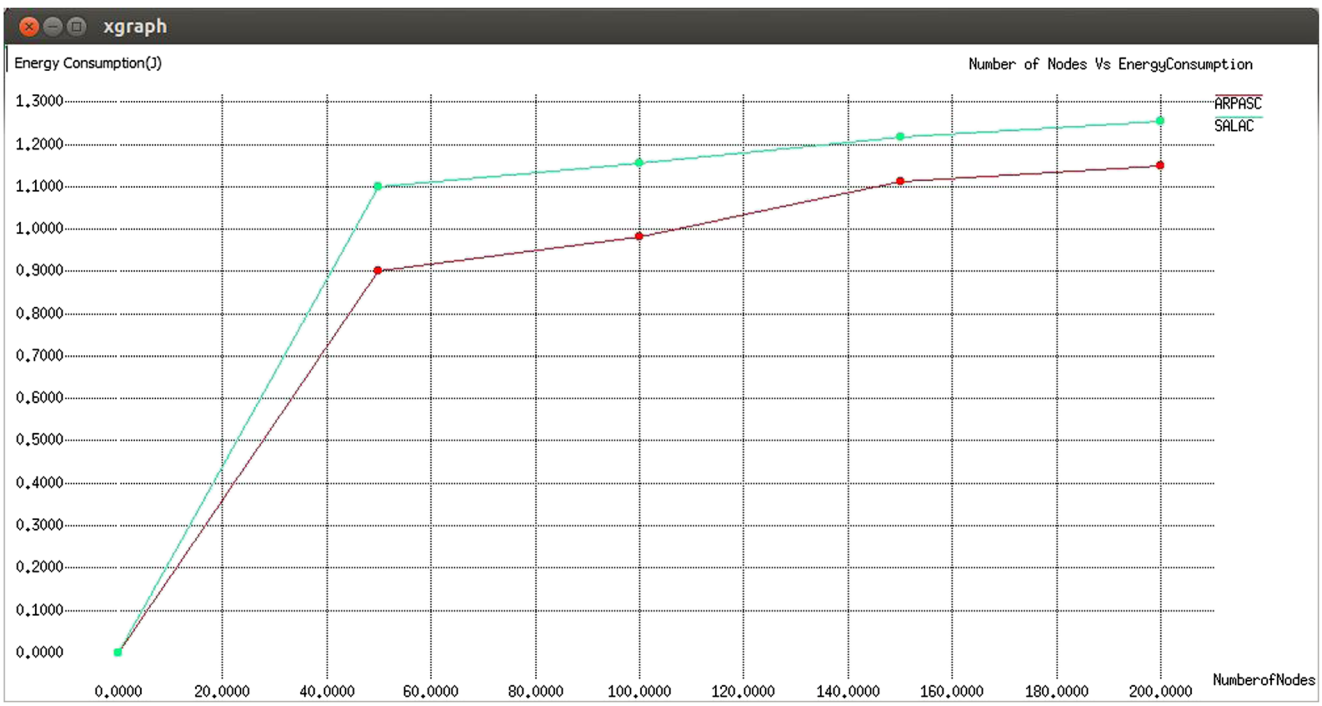

Fig. 9 Number of nodes vs energy consumption

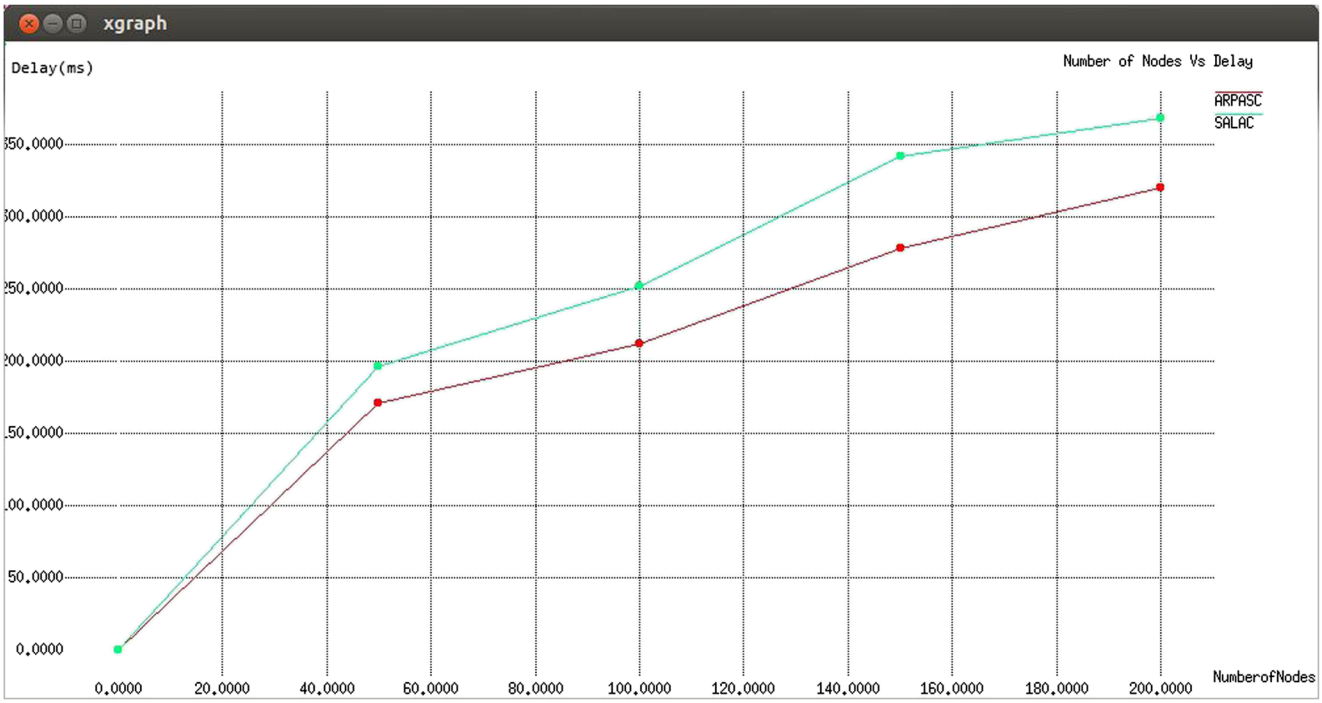

Fig. 10 Number of nodes vs end to end delay

We vary the number of attacks as 8,10 and 12 to analyze the performance.

Figure 3 shows the packet delivery ratio of ARPASC and SALAC techniques for different number of attacker scenario. In ARPASC, risk prediction and risk evidence improves the packet delivery ratio compared to SALAC protocol. We can conclude that the packet delivery ratio of our proposed ARPASC approach is 12.6% higher than SALAC approach.

Figure 4 shows the average throughput of ARPASC and SALAC techniques for different number of attacker scenario. In ARPASC chances of path failure is very less compared to SALAC resulting in better throughput compared to SALAC. It can observed that the average throughput rate of our proposed approach is 14.2% higher than SALAC approach.

Figure 5 shows the energy consumption of ARPASC and SALAC techniques for different number of attacker scenario. Overall energy consumption is less in ARPASC compared to SALAC due to less path failures. Adaptive risk prediction and risk evidence in the proposed technique results in 11.8% less energy consumption compared to SALAC approach. From Fig. 6 it can be concluded that the end-to-end delay of our proposed ARPASC approach is 16.4% less than SALAC approach.

Based on number of nodes

In our second experiment we vary the number of nodes as 50,100,150, and 200 and analyze the protocol performance.

In ARPASC, risk prediction and risk evidence improves the packet delivery ratio compared to SALAC protocol due to less path compromisation and less path failures. Figure 7 demonstrates that the packet delivery ratio of our proposed ARPASC approach is 14.7% higher than SALAC approach.

Figure 8 shows the average throughput of ARPASC and SALAC techniques for different nodes scenario. In ARPASC chances of path failure is very less compared to SALAC resulting in better throughput compared to SALAC. We can conclude that the throughput of our proposed ARPASC approach is 17.6% higher than SALAC approach.

Overall energy consumption is less in ARPASC compared to SALAC due to less path failures. It can be observed from Fig. 9 that the energy consumption of our proposed ARPASC approach is11.9% less than SALAC approach. Figure 10 demonstrates that the end to end delay of our proposed ARPASC approach is 12% less than SALAC approach.

Conclusion

In this paper, we proposed an Adaptive Risk Prediction and Anonymous Secured Communication protocol in MANET. The proposed technique can be applied for medical informatics where secured anonymous communications play a vital role. In this proposed technique, vulnerability path estimation is done by using hidden markoval model. We adopted the decision tree to determine the risk evidence and determine the attack level rate based on the risk estimation matrix table and vulnerability path rate data. We estimate the probability risk rate of adjacent nodes and paths to predict the attack probability in

anonymous environment. We employed anonymous secured message authentication scheme to enhance the security of anonymous communication. Experimental results demonstrate the efficiency of proposed Adaptive Risk Prediction and Anonymous Secured Communication model.

References

1. Koh, J. Y., Nevat, I., Leong, D., and Wong, W.-C., Geo-spatial location spoofing detection for Internet of Things. *IEEE Internet Things J.* 3(6):971–978, 2016.
2. Wang, C., Lin, H., and Jiang, H., CANS: Towards congestion-adaptive and small stretch emergency navigation with wireless sensor networks. *IEEE Trans. Mobile Comput.* 15(5):1077–1089, 2016.
3. Baiardi, F., Falleni, A., Granchi, R., Martinelli, F., Petrocchi, M., and Vaccarelli, A., Seas, a secure e-voting protocol: Design and implementation. *Comput. Secur.* 24(8):642–652, 2005.
4. Shepard, S. S., Dong, R., Kresman, R., and Dunning, L., Anonymous id assignment and opt-out. In: Ao, S., Gleman, L. (Eds), Lecture notes in electrical engineering. New York: Springer, 2010, 420–431.
5. Zhao, Z., Hu, H., Ahn, G.-J., and Wu, R., Risk-aware response for mitigating MANET routing attacks. *IEEE Transactions on Dependable and Secure Computing* 9(2), 2012.
6. Zhao, P., Li, J., Zeng, F., Xiao, F., Wang, C., and Jiang, H., ILLIA: Enabling k-anonymity-based privacy preserving against location injection attacks in continuous LBS queries. *IEEE Internet Things J.* 5(2), 2018.
7. Cui, J., Wen, J., Han, S., and Zhong, H., Efficient privacy-preserving scheme for real-time location data in vehicular ad-hoc network, 2327–4662 (c) IEEE, 2018.
8. Memon, I., Hussain, I., Akhtar, R., and Chen, G., Enhanced privacy and authentication: An efficient and secure anonymous communication for location based service using asymmetric cryptography scheme. New York: Springer Science+Business Media, 2017. https://doi.org/10.1007/s11277-015-2699-1
9. Sarathamani, T., and Babu, D. M. R., Robust and secure anonymity based routing protocol in manet. *Journal of Advanced Research in Dynamical and Control Systems* 9(6), 2017.
10. Xia, H., Li, Z., Zheng, Y., Liu, A., Choi, Y.-J., and Sekiya, H., A novel light-weight subjective trust inference framework in MANETs, IEEE transactions on sustainable computing, manuscript tsusc-2017-07-0063.
11. Cai, F., Ming, L., Jing, C., Li, Z., and Liu, X., A projection pursuit based risk assessment method in mobile ad hoc networks. *International Journal of Computational Intelligence Systems* 4(5): 749–758, 2011.
12. Liu, A., Joy, A., and Thompson, R., A dynamic trust model for mobile ad hoc networks. In: Proceedings of 10th IEEE Int'l Workshop Future Trends Of Distributed Computing Systems (Ftdcs '04), 80–85, 2004.
13. Dai, H., Jia, Z., and Kin, Z., Trust evaluation and dynamic routing decision based on fuzzy theory for MANETs. *Journal of Software* 4(10):1091–1101, 2009.
14. Zhang, Y., and Lee, W., Intrusion detection in wireless ad-hoc networks. In: Proceedings of the sixth annual international conference on mobile computing and networking, Boston, 2000.
15. Bhargava, S., and Agrawal, D., Security enhancements in AODV protocol for wireless ad hoc networks. Proceedings of Vehicular Technology Conference (VTC) Fall, 4:2143–2147, 2001.
16. Mishra, A., Nadkarni, A., and Patcha, A intrusion detection in wireless adhoc networks. *IEEE Wirel. Commun.* 11(1):48–60, 2004.
17. Takagi, H., and Kleinrock, L., Optimal transmission ranges for randomly distributed packet radio terminals. IEEE Trans. Commun. 32(3):246–257, 1984.
18. Cao, Y., and Xie, S. A position based beaconless routing algorithm for mobile ad hoc networks. Proceedings of the International Conference on Communications, Circuits and Systems 1(1):303–307, 2005.
19. Giruka, V., and Singhal, M., Angular routing protocol for mobile ad-hoc networks. IEEE international conference on distributed computing systems workshops. Columbus, OH. 2005.
20. Bing, W. U. et al., Network-based malcode detection technology. J. Commun.:87–91, 2007.
21. Ritchey, R. W et al., Using model checking to analyze network vulnerabilities. IEEE Conference on Security and Privacy, 2000.
22. Beaudoin, L. et al., Asset valuation technique for network management and security. IEEE Conference on Data Mining Workshops, 2006.
23. Shen, D. et al., Adaptive Markov game theoretic data fusion approach for cyber network defense. IEEE Conference on Military Communications, 2007.
24. Cardenas, A. A., Ramezani, V., and Baras, J. S., HMM Sequential Hypothesis Tests for Intrusion Detection in MANETs, U.S. Army Research Office under Award No. DAAD19–01-1-0494 t
25. Estahbanati, M. M., Rasti, M., and Hamami, S. M. S., A mobile ad hoc network routing based on energy and Markov chain trust
26. Das, S., Mukhopadhyay, A., Saha, D., and Sadhukhan, S., A Markov-Based model for information security risk assessment in healthcare MANETs. Springer Science+Business Media, LLC, 2017.
27. Kannan, A., Sathiyamoorthy, E., A decision tree-based rule formation with combined PSO-GA algorithm for intrusion detection system. In: International Journal of Internet Technology and Secured Transactions Vol 6, no: 186, 2016.
28. Cayirci, E., Ghergherehchi, R., Modeling cyber attacks and their effects on decision process. Proceedings of the 2011 Winter Simulation Conference.
29. Network simulator <http://www.isi.edu/nsnam/ns>.
30. Lu, H., Li, J., and Guizani, M., Secure and efficient data transmission for cluster-based wireless sensor networks. *IEEE Trans. Parallel Distrib. Syst.* 25(3):750–761, 2014.