Int J Wireless Inf Networks
DOI 10.1007/s10776-017-0373-0

Performance Analysis of Privacy Protection System During Data Transfer in MANETs

Bhawani Shanker Bhati[1] · **Pallapa Venkataram**[1]

Received: 15 May 2017 / Accepted: 20 September 2017

Abstract The openness of a Mobile Adhoc network (MANET) makes it vulnerable to various attacks that can breach privacy, and this demands a privacy protection system. In this paper, we propose a privacy protection system with flexible and adaptable policies to protect privacy during data transfer based on application and context attributes. We also provide the performance analysis model to test the suitability of policies for maintaining privacy, which is essential for the real-time implementation of this system in a resource-limited MANET. Finally, the proposed privacy protection system is compared with previous works using simulations, and the results obtained show the effectiveness of the proposed privacy protection system.

Keywords Performance analysis · Data transfer · Privacy policies · Mobile Adhoc network · Context

1 Introduction

The self-organizing, decentralized and infrastructure-less features of MANETs provide a promising solution for several real-world applications [1]. The nodes in a MANET function as both router and host, and communicate with other nodes which are not in its transmission range through intermediate nodes by establishing a route and then transferring the packets. Though nodes are considered to be trustworthy, however, a few nodes might be malicious and launch attacks to breach privacy [2]. Privacy requirement for MANET applications is challenging when compared to other applications because packets are transmitted over the wireless channel in multiple hops, which makes interception of the packet by attackers an easy task. Also, route maintenance due to frequent route and node failures increases the duration of data transfer, which can be utilized by attackers to launch attacks (like sender and receiver identification) by intercepting more packets.

Over the past decade, many privacy protecting systems have been proposed and analyzed, which are based on pseudonyms, masking information, privacy policies, etc. [3–5]. In particular, existing works on the analysis of privacy protection system based on policies have mainly focused on determining the redundancy, incompleteness, etc. [6], and have not concentrated on the suitability of these privacy policies. This paper analyzes the privacy protection system by analyzing the performance of privacy policies and also determine the suitability of privacy policies to preserve privacy in MANETs.

1.1 Need for Analyzing the Performance of Privacy Protection System

MANETs are often deployed in hostile environments where nodes' privacy needs to be safeguarded. The following reasons make analysis necessary:

- Minimizing the attacks on nodes in a MANET by eliminating the weaknesses and inaccuracies in privacy policies.
- Designing of privacy policies is an error-prone activity, and privacy policies are vulnerable to privacy breaches due to these errors.

✉ Pallapa Venkataram
pallapa@iisc.ac.in

Bhawani Shanker Bhati
bhati@iisc.ac.in

[1] Protocol Engineering and Technology Unit, Department of ECE, Indian Institute of Science, Bangalore 560012, India

Published online: 03 October 2017

- Privacy policies with low design complexities (i.e., time and space) are essential for smooth operation of resource-limited MANETs.
- It is also necessary to understand the effects of policy changes/updates.
- It is necessary to have transparent privacy policies to promote the acceptance of MANET applications by the general public.

As an important step towards achieving the necessities mentioned, we provide a model to analyze the privacy protection system in MANETs. The main contributions of this paper are summarized as follows:

- *Performance Analysis Model* A model is presented for analyzing privacy policies in privacy protection system during data transfer.
- *Complexity of Privacy Policies* Analysis of privacy policies for time and space complexity is discussed.
- *Behavioural of Intermediate Nodes*: Analyzing the cooperative nature of nodes en route to preserve privacy based on privacy policies.
- *Dependency of Privacy Policies on Context Attributes* Analyzing the dependence of privacy policies on context attributes, to determine the relevance and stability of privacy policy due to context awareness.

1.2 Organization of the Paper

The rest of the paper is organized as follows. In Sect. 2, some of the related works are summarized. Concepts and definitions are explained in Sect. 3. Section 4 discusses the proposed privacy protection system during data transfer. The detailed explanation of the performance analysis model is provided in Sect. 5. Section 6, discusses the simulation environment and obtained results. Finally, we conclude in Sect. 7.

2 Some of the Related Works

In literature, works have been done to analyze the policies, such as network management [7], power management [8], scheduling and dropping [9, 10], access control [11, 12], and privacy [13–15]. Most of the works on policy analysis have concentrated on detecting redundancy, similarity, weaknesses, trade-off, and incompleteness. For example, Soares et al. [9] investigates the efficiency and trade-off of scheduling and dropping policies in the routing. Similarly, Zheng et al. [8] presents an analytical model to characterize the energy-performance trade-off of various power management policies in wireless networks. Guarnieri et al. [16] deals with the redundancy removal in access control policies, and solve two problems, namely minimum policy problem and minimum irreducible policy problem. Rao et al. [17] provides EXAM, which is a comprehensive environment for analyzing a variety of functions such as policy property analysis, policy similarity analysis, and policy integration. The work in Lobo et al. [18], proposes policy similarity measure as a lightweight ranking approach to help one party quickly locate parties with potentially similar policies.

In the case of privacy policies, there have been works that concentrate on evaluating the awareness of privacy policies, such as Talib et al. [15] examines the perception of users towards privacy policies in social networks, where the focus is on evaluating privacy policy awareness among users. A comprehensive survey on policy analysis technique with a focus on access control policies and obligations for security and privacy is presented in [19]. For the web access control policies, Hongxin et al. [20] discusses a policy anomaly analysis approach and introduces a policy-based segmentation technique to accurately identify policy anomalies and derive effective anomaly resolutions. Fisler et al. [12] presents a suite called Margrave for analyzing access control policies written in the XACML standard. Duan et al. [13] presents a privacy disclosure recommendation approach based on a privacy cost model, where appropriate attributes are selected from users to automatically build a new credential for authorization policies. Privacy policies are derived automatically by analyzing the user's sharing behaviour [14], and then validated by implementing it as an extensible software library for the Android platform and developing plug-ins for collaboration tools. Similarly, Bakar et al. [5] combines the access control mechanism and privacy policy to protect personal data during emergency services, and further provide an android mobile application which integrates the privacy access model [21]. Aldabbas et al. [22] attaches the originator policies to the data packets while data transfer to provide privacy and data confidentiality. However, Aldabbas et al. [22] do not focus the performance of the system during data transfer. Chen et al. [23] proposes a Trusted Anonymous Routing (TARo) protocol, and also propose mechanisms for the selection of trusted router. TARo provides an anonymous data transfer to preserve the identity of nodes, and send a route error (*rerr*) message to the sender for route maintenance. Aviv et al. [24] designs a privacy-aware geographic routing protocol to allow message exchanges in decentralized human movement networks consisting of smartphones. During message exchange, it minimizes the undesired exposure of sensitive information. Miller et al. [25] considers metric that takes all aspects of privacy implementation from the perspective of usability to improve user privacy outcomes. To detect malicious nodes in a MANET, Li et al. [26] proposes

CAST, where policies are defined based on the context information to distinguish malicious nodes from malfunctioning nodes. We see that in most of the existing works on privacy policy analysis mainly concentrate on examining user awareness, policy anomalies, etc., however, performance analysis of privacy policies are not much explored.

3 Concepts and Definitions

In this section, we discuss the concepts and definitions used. We provide the details on: (1) Attributes considered for designing the privacy policy; (2) Acquisition of attributes; (3) Privacy policy design based on the attributes; and (4) Rough set theory concepts for privacy protection.

3.1 User Context Attribute and Application Attribute

The user context attributes (*Usr_CA*) specifies the user's concern towards privacy. We consider following user context attributes: Experience, Status, Interest, Goal, Connectivity and Device Safety. The Connectivity specifies whether user's neighborhood can preserve privacy or not, and it is measured as a number of neighbors. The Device Safety specifies the capability of a user's device to maintain privacy, and it is dependent on whether user's device includes protection mechanisms or not such as given in [27]. Table 1, shows the value that can be taken by *Usr_CA*. Experience (respectively, Connectivity) takes value within a range with pre-defined minimum E_{min} (respectively, C_{min}), maximum E_{max} (respectively, C_{max}) and threshold E_{th} (respectively, C_{th}). If user's Experience (respectively, Connectivity) is below E_{th} (respectively, C_{th}) then Experience (respectively, Connectivity) is low (=1), and if it is above E_{th} (respectively, C_{th}) then Experience (respectively, Connectivity) is high (=3). For example, if a user belongs to the banking community, then Experience can take values within [0,30] years (where, [0,15] = Low and (15,30] = High), Status can take values {clerk, manager} (where, clerk = Low and manager = High), Interest can take values {bank's employee benefits, financial statements} (where, bank's employee benefits = Insensitive and financial statements = Sensitive), Goal can take values {opening an account, loan-clearance} (where, opening an account = Short term and loan-clearance = Long term), Connectivity can take values within [0,10] neighbors (where, [0,5] = Low and (5,10] = High), and Device Safety can take values {no, yes} (where, no = Low and yes = High).

Applications require a different level of privacy maintenance, and it is determined using application attributes representing application's sensitivity (*AA*). The *AA* is determined only by a sender (who establishes a route for a particular application) based on the following application attributes: Criticality (*CR*), Session Impact (*SI*), and Traffic Impact (*TI*). Criticality defines application type; Session Impact indicates the impact of sessions in an application, i.e., number and duration of the session; and Traffic Impact represents the application's traffic impact, i.e., traffic size and frequency. Table 2, shows the values taken by application attributes, where each application attribute takes value within a range with pre-defined minimum i_{min}, maximum i_{max} and threshold i_{th} for $i \in \{CR, SI, TI\}$. We mention that, context and application attributes can take finer values, however, for simplicity, we have assigned the values as shown in Tables 1 and 2, respectively.

Table 1 User context attribute values

Experience	Status	Interest	Goal	Connectivity	Device safety
$[E_{min},E_{th}]$	L	IS	ST	$[C_{min},C_{th}]$	L
$[E_{min},E_{th}]$	L	IS	ST	$[C_{min},C_{th}]$	H
$[E_{min},E_{th}]$	L	IS	LT	$[C_{min},C_{th}]$	L
..	..	..	..	..	..

L: low (= 1), H: high (= 3), IS: insensitive (= 1), S: sensitive (= 3), ST: short term (= 1), LT: long term (= 3)

3.2 Context Attributes Acquisition

To provide confidentiality during the acquisition of context attributes, nodes use t-degree polynomial functions [28] to privately send their context. Context information is also acquired while establishing a route and data transfer. Initially, during route establishment stage, context attributes value is attached with the route request/route reply (*rreq*/*rrep*) messages by every trusted node, which is selected based on the trust attributes [29], and during data transfer, context attribute values are piggybacked along with the data packet. We assume that every node has a Context

Table 2 Application attribute values

Criticality	Session impact	Traffic impact	*AA*
$[CR_{min}, CR_{th}]$	$[SI_{min}, SI_{th}]$	$[TI_{min}, TI_{th}]$	Low = 1
$[CR_{min}, CR_{th}]$	$[SI_{min}, SI_{th}]$	$(TI_{th}, TI_{max}]$	Medium = 2
$[CR_{min}, CR_{th}]$	$(SI_{th}, SI_{max}]$	$[TI_{min}, TI_{th}]$	
$(CR_{th}, CR_{max}]$	$[SI_{min}, SI_{th}]$	$[TI_{min}, TI_{th}]$	
$[CR_{min}, CR_{th}]$	$(SI_{th}, SI_{max}]$	$(TI_{th}, TI_{max}]$	High = 3
$(CR_{th}, CR_{max}]$	$[SI_{min}, SI_{th}]$	$(TI_{th}, TI_{max}]$	
$(CR_{th}, CR_{max}]$	$(SI_{th}, SI_{max}]$	$[TI_{min}, TI_{th}]$	
$(CR_{th}, CR_{max}]$	$(SI_{th}, SI_{max}]$	$(TI_{th}, TI_{max}]$	

Collector Module (CCM), which is responsible for communicating with the sensors available on the device (like GPS, processing unit, battery unit, buffer unit, etc.). The CCM sends the context information using the t-degree polynomial functions, *rreq/rrep* messages, and by piggybacking during data transfer. In the case of t-degree polynomials, node should be aware of the functions $f_{n,k}(x)$, where first index and second index represents destination node-id (n, i.e., node receiving context) and source node-id (k, i.e., node sending context), respectively. The format of packet for context acquisition is: <node-*s*, *Context_Attribute*, *Parameter*, *Value*>. For example, when a node-*a* in area of trusted intermediate node-*n* sends its dynamic context information, it sends out an encrypted packet $E_{f_{n,a}(a)}$ (node-*a*, *Usr_CA*, *Connectivity*, *4*), which indicates that 'node-*a*' has sent 'Connectivity' parameter of 'User Context Attribute' having value '4'. When node-*n* receive this information, it makes an entry in its Context Information Table (CIT). We mention that context attributes parameter are updated whenever their value changes. For example, neighborhood connectivity is updated if a number of nodes moved/entered within the transmission range of a node is greater than a pre-defined value. In rest of the paper, we call *'context messages'* as the messages that contain context attribute values, and are sent using t-degree polynomial function, *rreq*, *rrep*, and piggybacking. Since *AA* determine the application sensitivity, thus, application attributes are not maintained in a CIT. Algorithm 1, presents the details on the acquisition of context attributes during route establishment and data transfer. Based on these acquired context information, privacy policies are designed for each of the trusted nodes en route.

3.3 Privacy Policy Design

Policies are designed for each of the trusted intermediate node on an established route based on context attribute and application attribute, which define tasks (to be performed by nodes en route) in order to maintain privacy. The tasks are: determining type of next hop node in terms of privacy maintenance (t1), and permitting next hop node to re-establish route, i.e., local repair, with or without sending a route error (*rerr*) message to sender (t2) in case of failure detection. Thus, privacy policy is represented as tuple (similar to [6], but in this paper, we consider attributes and tasks) containing attributes (A) and tasks (Ta), i.e., [A, Ta]. The examples for privacy policy are as follows:

1. *[Experience == (15,30]* $\wedge$ *Status == H* $\wedge$ *Interest == IS* $\wedge$ *Goal == ST* $\wedge$ *Connectivity == (5,10]* $\wedge$ *Device Safety == H* $\wedge$ *AA == L]*, *[Type of node = Lowest privacy maintenance*, *Route re-establishment = Allow local repair without informing sender].*
2. *[Experience == [0,15]* $\wedge$ *Status == L* $\wedge$ *Interest == S* $\wedge$ *Goal == LT* $\wedge$ *Connectivity == [0,5]* $\wedge$ *Device Safety == L* $\wedge$ *AA == H]*, *[Type of node = Highest privacy maintenance*, *Route re-establishment = Allow local repair with informing sender].*

In (1), user has high Experience, high Status, insensitive Interest, short term Goal, high Connectivity and high Device Safety, with lower Application Sensitivity (or AA). For this, the node has lowest privacy maintenance and initiates local route re-establishment without informing the sender. However, in (2), the node has highest privacy maintenance, and sender needs to be informed about route

Algorithm 1 Pseudo-code for Acquisition of Context Attributes

```
Begin
Sender initiates route establishment
/* Acquiring context during route establishment */
while Not receiver do
    for all Trusted neighbor nodes do
        nodes acquire the context using t-degree polynomial function
        /* E_{f_{a,s}(s)}(node-s, Context_Attribute, Parameter, Value); from node-s to node-a */
    end for
    for Trusted intermediate node do
        context acquisition using rreq and rrep messages
        /* node-(n) ⇄^{rreq}_{rrep} node-(n+1); context acquisition between nodes n and (n+1)*/
    end for
end while
if Route is established between sender and receiver then
    Sender initiates the data transfer
    /* Acquiring context during data transfer */
    while Data transfer not complete do
        for all Trusted neighbor nodes do
            nodes acquire the context using t-degree polynomial function
        end for
        for Trusted intermediate node do
            acquire the updated context by piggybacking with data packet
            /* node-(n) --data+ context--> node-(n+1); from node-(n) to node-(n+1) */
        end for
    end while
end if
End
```

re-establishment. The privacy maintenance for each node on an established route is determined based on attributes by applying rough set concepts.

3.4 Rough Sets

Rough set theory, introduced in early 1980's [30] is used extensively in various fields, mainly for reasoning about knowledge and classification. The data is represented using an information table, denoted as $I = <U_{No}, A_C, V, f>$, where U_{No} is a non-empty finite set of objects called universe, A_C is a non-empty finite set of attributes, $V = V_{c_1} \cup V_{c_2} \cup \ldots V_{c_C}$ (V_{c_i} is the value of the attribute 'c_i') and 'f' is an information function which appoints the attribute value to every object in U_{No}. Table 3 represents set of nodes as universe and their context attributes as set of attributes. Rough set concepts, use the context information to classify the nodes into three separate regions: positive region (PosR), negative region (NegR) and boundary region (BndR), based on context attributes. Considering, $T \subseteq A_C$ and $Y \subseteq U_{No}$, then the approximation of Y is determined based on the information in T, by finding *T-lower* ($T_l(Y) = \{e \in U_{No} | [e]_T \subseteq Y\}$) and *T-upper* ($T_u(Y) = \{e \in U_{No} | [e]_T \cap Y \neq \phi\}$) approximations of Y. $[e]_T$ is the equivalence classes of *T-indiscernibility* relation. The nodes in $T_l(Y)$ can be certainly the elements of Y and the nodes in $T_u(Y)$ can be possible elements of Y, based on the context attributes in T. Using the $T_l(Y)$ and $T_u(Y)$, universe U_{No} is divided into three disjoint regions: (1) *Positive region*, $\text{PosR}(Y) = T_l(Y)$; (2) *Negative region*, $\text{NegR}(Y) = U_{No} - T_u(Y)$; and (3) *Boundary region*: $\text{BndR}(Y) = T_u(Y) - T_l(Y)$. In this paper, we define 'PosR' as nodes which are highly reliable in terms of privacy maintenance, 'NegR' as nodes which are not (lowest) reliable and 'BndR' as nodes which have medium reliability in terms of privacy maintenance. However, we mainly focus on nodes in the positive region for privacy protection.

4 Privacy Protection During Data Transfer

In MANETs, a sender initiates data transfer after establishing a route to a receiver, via intermediate nodes. To avoid leakage of information, we consider an established untraceable route on a hop-by-hop basis through trusted intermediate nodes [29]. During data transfer, these trusted intermediate node may fail to preserve privacy, which can be due to reasons such as: (1) Moving out of transmission range, and/or (2) Not able to maintain the privacy of a sender's application (i.e., a decrease in context attribute value). Thus, privacy protection during data transfer is proposed. First, we give details on the construction of context information table, and finally, present the proposed privacy protection system during data transfer in detail.

4.1 Context Information Table

The context attribute acquired during route establishment and data transfer stages are maintained in CIT at trusted nodes en route. In CIT, rows represent the node-ids, and each column represents their context attribute. The values in CIT are updated, whenever there is a change in the context of any neighbor. Table 4 shows an example of CIT at node-C with n_1, n_2, n_3, n_4, n_5 as the node-id of next hop nodes (trusted neighbor of node-C towards receiver) and columns represents their context attributes.

4.2 Proposed Privacy Protection During Data Transfer

At each routing step, data transferring node applies the rough set theory concepts to determine privacy maintenance level of next hop node based on it's context attributes and sender's application attributes. Then, based on privacy maintenance level of next hop node, violations to preserve privacy are identified. Finally, if privacy violation is detected, then a route is locally repaired (with/without informing sender) by selecting an alternate trusted intermediate node from neighbour nodes of data transferring node. This complete process is continued till the receiver node. Now, we discuss how: (1) privacy maintenance level is determined; (2) privacy losses are detected; and (3) efficiently route is re-established with privacy maintenance.

First, privacy maintenance level of a trusted intermediate node, say node-l (denoted as M_l) is given as in Eq. 1.

$$M_l = \alpha * M_l^{AA} + (1 - \alpha) * M_l^{CIT} \quad (1)$$

where, α is the self-weightage factor (to be set high to increase self weightage), M_l^{AA} represents privacy maintenance level calculated from the sender's application sensitivity, and M_l^{CIT} represents privacy maintenance level

Table 3 Rough set concept for privacy protection system

Symbol	Definition
$U_{No} = \{n_1, n_2, \ldots, n_{No}\}$	Non-empty finite set of nodes
$A_C = \{c_1, c_2, \ldots, c_C\}$	Non-empty finite set of context attributes {*Experience, Status, Interest, ..*}
V_{c_i}	Value of the context attribute 'c_i'

Table 4 CIT at node-*C*

node-*C*	*Experience*	*Status*	*Interest*	*Goal*	*Connectivity*	*Device Safety*
n_1	1	1	3	1	1	1
n_2	3	3	1	1	1	1
n_3	1	1	1	3	1	1
n_4	3	1	1	1	1	3
n_5	3	1	1	3	3	1

calculated from the node-l context attributes which are obtained from the CIT. $M_l^{AA} = \frac{1}{AA}$ and $M_l^{CIT} = \sum_j (W_l^{CIT}(j) * V_l^{CIT}(j))$, where, AA is the value of sender's application sensitivity, $j \in \{Experience, Status, Interest, Goal, Connectivity, Device\ Safety\}$, $W_l^{CIT}(j)$ and $V_l^{CIT}(j)$ are the weights and values of context attribute-j of node-l. A trusted intermediate node requires sender's application sensitivity to determine privacy maintenance level for next hop. Since, sender desires to preserve application privacy (i.e., not revealing the application for which a route is established), thus sender sends a quantized value of application sensitivity (for example, AA = 3, indicating highly sensitive application) with the *rreq* message during route establishment stage.

Second, to detect privacy loss by next hop node, a check time ($T_c = \lceil log(N_{dp} * M_l) \rceil$) is determined, where N_{dp} is the number of data packets to be transfer to next hop node, i.e., data transferring node performs a check after transferring every T_c number of data packets, to identify any changes in next hop node's behaviour and the link between them. A low T_c implies that there is a need to check the next hop node very frequently, whereas a high T_c indicates a lesser number of checks during data transfer. We mention that only trusted intermediate nodes en route, periodically checks whether privacy is maintained by their next hop node. A check, $U(T_c) = \eta * E(T_c)$ is performed by determining the change in privacy maintenance level. $U(T_c)$ is the change in privacy maintenance level at T_c, $E(T_c)$ is the difference between current and previous privacy maintenance level and η is a proportional constant. If the change is within a predefined value then data transfer is continued, otherwise transferring node detects a failure to maintain privacy (by next hop) and selects another trusted intermediate node for data transfer by initiating route recovery. The privacy maintenance level can change due to changes in dynamic context attribute: (1). Connectivity—since the change in neighbourhood connectivity effects privacy by reducing untraceability of a route and thus reducing the computational overhead of an attacker; and (2) User's Experience—since it reflects the trusted intermediate node's attitude towards privacy. We also check for: (1) dropping of packets and not notifying using *rerr* message—since it reflects a malicious activity of a node; and (2) node moving out of transmission range.

Third, an efficient route re-establishment scheme avoids privacy breach by minimizing the delay and choosing another trusted intermediate node for data transfer which can maintain privacy. For this, the node detecting the failure establishes a connection with any of its trusted neighbour node (towards receiver), and if, there are no trusted neighbours, then node initiates route re-establishment with/without sending an acknowledgement (in the form of *rerr* message) to a sender. To reduce the overhead during route re-establishment stage, sender and trusted intermediate nodes consider only those nodes which are highly trusted and have higher privacy maintenance level, i.e., nodes within the positive region (see Sect. 3.4).

5 Performance Analysis

In this Section, we discuss the performance of privacy protection system by analyzing the performance of designed privacy policies. First, we give details on performance analysis model, and later, we theoretically analyze the privacy policies.

5.1 Performance Analysis Model

Performance analysis model consists of following modules (as shown in Fig. 1): *Complexity Analysis*, *Behavioral Analysis of Intermediate Node* and *Dependency Analysis on Context Attribute*. Each module defines performance metrics for analyzing the privacy policies, and details are given in Sects. 5.2, 5.3 and 5.4, respectively.

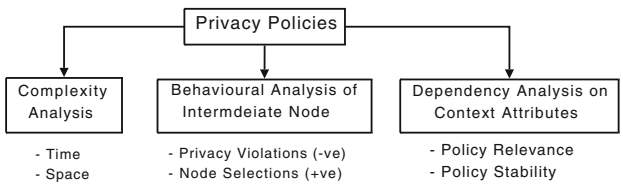

Fig. 1 Performance analysis model

5.2 Complexity Analysis

Analyzing the complexity introduced on nodes due to dynamic privacy policies during data transfer, and it is essential in the case of resource-limited MANET nodes. The performance metrics for *Complexity Analysis* are: *Time Complexity* and *Space Complexity*.

5.2.1 Time Complexity

It is the time required by nodes en route to design a privacy policy comprising of attributes and tasks. Thus, time complexity depends on: (1) time required for identifying context attributes (T_{ca}) which are received through *context messages*; and (2) time required to determine the respective tasks (T_{ta}). Application attributes are not considered since they are received during route establishment stage. For simplicity of analysis, we consider that *context messages* are arriving at a node with rate 'γ' messages/s. Then, total number of *context messages* arrived (N_{ma}) is, $N_{ma} = \gamma * D_{dt}$, where D_{dt} is the data transmission duration, and N_{ma} accounts for the total time complexity during data transfer which includes multiple privacy policy updates. Assuming a constant time, t_{pf} to be the time required to read and identify the contents of *context messages*, then $T_{ca} = t_{pf} * N_{ma}$. We mention that N_{ma} does not reflect the number of privacy policy changes during data transfer, since, policies are not changed (or updated) for every *context messages* received.

To determine number of changes in privacy policy during data transmission duration, we assume that a privacy policy is changed only after receiving n_{dc} number of different context attribute. So, average number of privacy policy changes (N_{ppu}) is given by Eq. 2.

$$N_{ppu} = \frac{PU_{max} + PU_{min}}{2} \tag{2}$$

where, PU_{min} and PU_{max} are the minimum and maximum number of expected policy changes (denoted as PU). PU is determined as, $PU = N_{ma} * \binom{N_{da}}{y} * (p_{dc})^{y} * (1 - p_{dc})^{N_{da}-y}$, where $y \in \{1, 2, \ldots, N_{da}\}$, $N_{da} = \lfloor \frac{N_{ma}}{n_{dc}} \rfloor$, $p_{dc} = \prod_{i=1}^{n_{dc}} p_i$, and p_i is the probability of changing ith context attribute value.

For every change in privacy policy, tasks are determined by using *if-else* statements (see privacy policies in Sect. 3.3). Then, we have $T_{ta} = t_{if} * N_{ppu}$, where t_{if} is the time complexity of one *if-else* statement. The t_{if} depends on number of context attribute (denoted as N_c) which are considered for designing privacy policies and processing speed of a node (denoted as P_s), i.e., $t_{if} = \frac{N_c * L_{ca}}{P_s}$, where L_{ca} is the length (in bits) of each attribute. Using T_{ca} and T_{ta}, we obtain the average time complexity for designing a privacy policy as given by Eq. 3.

$$C_{time} = \frac{T_{ca} + T_{ta}}{N_{ppu}} \tag{3}$$

5.2.2 Space Complexity

It is the storage requirement for privacy policies at each node en route, i.e., the space requirement for context attribute parameters and tasks. The space required to store context attribute is $S_{ca} = N_{ma} * L_{ca}$ bits. We have considered two tasks: *Type of Node* and *Route Re-establishment*, and we assume that the storage requirement for task *Type of Node* and task *Route Re-establishment* are 2 bits and 1 bit, respectively. Then storage requirement for tasks are $S_{ta} = 3 * N_{ppu}$. Using S_{ca} and S_{ta}, we obtain the average space complexity for designing a privacy policy as given by Eq. 4.

$$C_{space} = \frac{S_{ca} + S_{ta}}{N_{ppu}} \tag{4}$$

5.3 Behavioural Analysis of Intermediate Nodes

Analyzing the behaviour of trusted intermediate nodes to comply with privacy policies, and it is essential due to cooperative nature of nodes. It reflects the strength of privacy policies to preserve privacy in MANETs. The behaviour is determined by considering the following performance metrics: *Number of Policy Violation*—indicates negative i.e., selfish or malicious behaviour, and *Number of Node Selections*—indicates positive behaviour i.e., success of privacy policy. We mention that the negative behaviour of a trusted intermediate node during data transfer leads to selection of another node which consumes more time and is advantageous for an attacker. The behavioural analysis (change in behaviour) of an intermediate node is modelled as Discrete Time Markov Chain (DTMC) as shown in Fig. 2, where N, F, and P are the states representing negative, failed and positive behaviour, respectively. Dynamically changing privacy policies during data

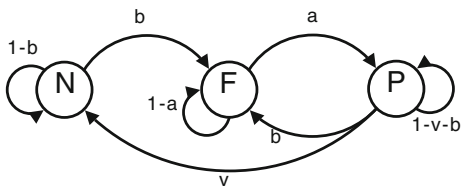

Fig. 2 State transition diagram for behaviour of an intermediate node

transfer reflects the change in node's behaviour, and we see that the privacy policy is changed due to genuine failure of a node (failed due to decrease in value of n_{dc} attribute, such as Connectivity) or privacy violation by a node (not able to perform privacy tasks). For simplicity, we assume that the node's behaviour is improved if there is an improvement in the privacy maintenance level, which is dependent on attributes. Considering a, b and v to be the probabilities of improvement (positive behaviour), genuine failure, and privacy violation, respectively. Since, each dynamic attributes value lies within $[j_{min},j_{max}]$, where $j \in \{E, C\}$, the probabilities a and b are determined as given by Eq. 5.

$$b = \prod_{j}(1 - p_j) \qquad a = 1 - b \tag{5}$$

where, $p_j = \frac{j_{max} - j_n}{j_{max} - j_{min}}$ is the probability that the node's behaviour improves due to increase in jth dynamic context attribute, j_n represents the dynamic context attribute of node-n, and $j \in \{C, E\}$.

To determine the probability of privacy violation (v), we mention the tasks that violate privacy: (1) not maintaining required privacy maintenance level; (2) violating route re-establishment task; (3) dropping packets without sending an acknowledgement; and (4) delaying packets. First two are related to violation in privacy maintenance tasks (T_{pm}), and the last two are related to violation in general tasks (T_{gn}) which can cause privacy breach by giving advantage to an attacker. Thus, probability of privacy violation (v) is given by Eq. 6, where $p_{T_{pm}}$ and $p_{T_{gn}}$ are probability of privacy violations due to privacy maintenance tasks and general tasks, respectively.

$$v = \frac{p_{T_{pm}} + p_{T_{gn}}}{2} \tag{6}$$

The work mainly focusses on determining $p_{T_{pm}}$, however, we also give details on determining $p_{T_{gn}}$. The $p_{T_{pm}}$ is determined based on the tasks: *Type of Node* and *Route Re-establishment*. For the task *Type of Node*, we assume that privacy maintenance level lies within $[M_{min}, M_{max}]$, where M_{min} and M_{max} are the minimum and maximum values, respectively. The probability with which a node's privacy maintenance level decreases (p_{pml}) is given as, $p_{pml} = 1 - (\frac{M_{max} - M_n}{M_{max} - M_{min}})$, where M_n is the privacy maintenance level for node-n. The task *Route Re-establishment* is related to repairing of route with (w)/ without (o) informing sender node. Thus, in this case privacy is violated if a node performs task which is opposite to required task, i.e., instead of performing o, the node performs w or vice-versa. Thus, probability of violating task *Route Re-establishment* is $p_{rr} = \frac{p_{wo} + p_{ow}}{2}$. The first and second index of p_{wo} and p_{ow}, indicates the actual task performed and required task that was needed, respectively. For simplicity of analysis, p_{wo} and p_{ow} are assumed to be equal, i.e., $p_{rr} = p_{wo}$. To determine p_{wo}, we use trustworthiness of a node (as given in [29]), i.e., a highly trusted node will less likely violate the task whereas a lower trusted node will more likely violate the task. Consider that trustworthiness lies between $[TV_{min},TV_{max}]$, then $p_{rr} = p_{wo} = (\frac{TV_{max} - TV_n}{TV_{max} - TV_{min}})$, where TV_n is the trustworthiness of node-n. So, probability of privacy violations due to privacy maintenance tasks is given by Eq. 7.

$$p_{T_{pm}} = p_{pml} * p_{rr} \tag{7}$$

The probability of privacy violation due to general tasks, $p_{T_{gn}}$ is determined based on: packet drop and packet delay. In literature, there have been works done to determine probability of packet drop and packet delay [29, 31]. Considering p_{DrP} and p_{DeP} to be the probability of dropping packets and delaying packets, respectively. Then probability of privacy violations due to general tasks is given by Eq. 8.

$$p_{T_{gn}} = p_{DrP} * p_{DeP} \tag{8}$$

From the DTMC model, we compute steady-state probabilities π_j, $j \in \{N,F,P\}$. To validate, we consider a Markov chain as represented in Fig. 2, where events are considered to arrive with rate γ to simulate change in values of attributes. Finally, from the steady state probabilities we determine the *Number of Policy Violation* by calculating the number of visits to state-N (denoted as V_N) when we start from other states, i.e., $V_N = (v * V_{PN}) + ((1 - b) * V_{NN})$. V_{PN} and V_{NN} represents the expected number of visits to state-N if we start in state-P and state-N, respectively. Similarly, we determine the *Number of Node Selections* (denoted as V_P) as, $V_P = (a * V_{FP}) + ((1 - b - v) * V_{PP})$. V_{FP} and V_{PP} represents the expected number of visits to state-P if we start in state-F and state-P, respectively.

5.4 Dependency Analysis on Context Attribute

The dependence of privacy policies on context attribute indicates the feasibility of context awareness in MANETs for privacy preservation. The following metrics are considered: *Privacy Policy Relevance* and *Privacy Policy Stability*.

5.4.1 Privacy Policy Relevance

Initially, privacy policies are designed after the route establishment, however, due to dynamic nature of the attributes, privacy policies are dynamically updated during data transfer. Thus, *Privacy Policy Relevance* is the

measure of ability of privacy policy to remain active, i.e., ability of jth privacy policy to remain active, before $(j+1)$th privacy policy is designed during transfer. Since, privacy policy is dependent on context attributes, *Privacy Policy Relevance* (R_i) is determined by using the following factors: freshness (f_c)—indicates up-to date, precision (p_c)—indicates exactness, source credibility (sc_c)—indicates trustworthiness of source, and availability uncertainty (CU_{avl})—indicates availability, of context attribute value, and given by Eq. 9.

$$R_i = \frac{f_c * p_c * sc_c}{CU_{avl}} \tag{9}$$

Now, we calculate f_c, p_c, sc_c, and CU_{avl}. For freshness, we assume that each context attribute value is valid till $[t_{min},t_{max}]$, thus freshness of context attribute is given by trapezoidal function (see Eq. 10).

$$f_c = \begin{cases} 0 & t_v \geq t_{max}, \\ 1 & t_v \leq t_{min}, \\ \dfrac{t_{max} - t_v}{t_{max} - t_{min}} & Else. \end{cases} \tag{10}$$

The privacy policies are designed by using discretized values of context attribute, which are defined based on finite number of intervals. In this case, precision is defined as the smallest difference between interval values (left and right boundary points of an interval) and the actual value for a particular context attribute. The precision of context attribute is given by Eq. 11, where a_j^n, r_j^n and l_j^n represents the actual value, right boundary point, and left boundary point for interval J of nth context attribute, respectively.

$$p_c = \min_i \{|r_j^n - a_j^n|, |l_j^n - a_j^n|\} \tag{11}$$

The source credibility is given by, $sc_c = \frac{TV_n}{TV_{max}}$ (determined by the trustworthiness of context source). Availability uncertainty (CU_{avl}) is the ratio of available context attribute (N_{avl}) to total context attributes (N_c), and it is given as, $CU_{avl} = 1 - \frac{N_{avl}}{N_c}$.

5.4.2 Privacy Policy Stability

The rough set theory concepts are employed over the context attribute-value pairs to determine privacy maintenance tasks, which in turn forms the privacy policy. The context attribute values are partitioned into finite number of intervals based on pre-defined threshold values of each context attribute parameter. The stability measure defined in [32] is used to determine the stability of rules (i.e., privacy policies) in rough set theory. From Beynon [32], probability density function for each of the intervals (of context attribute) is given by Eq. 12.

$$DF_{n,j}(x) = \frac{1}{\sqrt{2m_{n,j}\pi}} \sum_{i=1}^{m_{n,j}} \frac{1}{r_j^n - l_j^n} exp\left[-\frac{1}{2}\left(\frac{x - x_i}{r_j^n - l_j^n}\right)^2 \right] \tag{12}$$

where, $m_{n,j}$ is the number of objects in the I_j^n interval, I_j^n is defined as the jth interval of nth context attribute. The stability index measure for an interval is given by Eq. 13, where $P_{n,j,j}$, $\underline{P}_{n,j}$ and $\overline{P}_{n,j}$ are probability of a value from the nth context attribute categorized as in the jth interval is categorized correctly to the jth interval, lower bounds on $P_{n,j,j}$ and upper bounds on $P_{n,j,j}$, respectively. The upper and lower bound are given as, $\underline{P}_{n,j} = \int_{l_j^n}^{r_j^n} \underline{DF}_{n,j} dx$ and $\overline{P}_{n,j} = \int_{l_j^n}^{r_j^n} \overline{DF}_{n,j} dx$, and Eqs. 14 and 15 defines $\underline{DF}_{n,j}$ and $\overline{DF}_{n,j}$, respectively, where k_n indicates the number of intervals.

$$SI_{n,j} = \frac{P_{n,j,j} - \underline{P}_{n,j}}{\overline{P}_{n,j} - \underline{P}_{n,j}} \tag{13}$$

$$\underline{DF}_{n,j} = \begin{cases} \sqrt{\dfrac{m_{n,j}}{2\pi}} \dfrac{1}{r_j^n - l_j^n} exp\left[-\dfrac{m_{n,j}}{2}\left(\dfrac{x - r_j^n}{r_j^n - l_j^n}\right)^2 \right] \\ \qquad j = 1, \ldots k_n - 1 \\ \sqrt{\dfrac{m_{n,j}}{2\pi}} \dfrac{1}{r_j^n - l_j^n} exp\left[-\dfrac{m_{n,j}}{2}\left(\dfrac{x - l_j^n}{r_j^n - l_j^n}\right)^2 \right] \\ \qquad j = k_n \end{cases} \tag{14}$$

$$\overline{DF}_{n,j} = \begin{cases} \sqrt{\dfrac{m_{n,j}}{2\pi}} \dfrac{1}{r_j^n - l_j^n} exp\left[-\dfrac{m_{n,j}}{2}\left(\dfrac{x - 0.5(r_j^n + l_j^n)}{r_j^n - l_j^n}\right)^2 \right] \\ \qquad j = 2, \ldots k_n - 1 \\ \sqrt{\dfrac{m_{n,j}}{2\pi}} \dfrac{1}{r_j^n - l_j^n} exp\left[-\dfrac{1}{2}\left(\dfrac{m_{n,j}x - \sum_{i=1}^{m_{n,j}} x_i}{r_j^n - l_j^n}\right)^2 \right] \\ j = 1, k_n \end{cases} . \tag{15}$$

Context attribute stability index (SI_{cap}) is calculated using

Table 5 Analysis and simulation parameters

Parameter	Value (s)
Number of nodes	400
Transmission range	200 m
Node mobility	Varying (m/s)
Mobility model	Random way point
$C_{min,th,max}$	{0, 5, 10}
$CR_{min,th,max}$	{1, 2, 3}
$SI_{min,th,max}$	{1, 2, 3}
$TI_{min,th,max}$	{1, 2, 3}
N_c	Varying
$[TV_{min}, TV_{max}]$	[1,3]

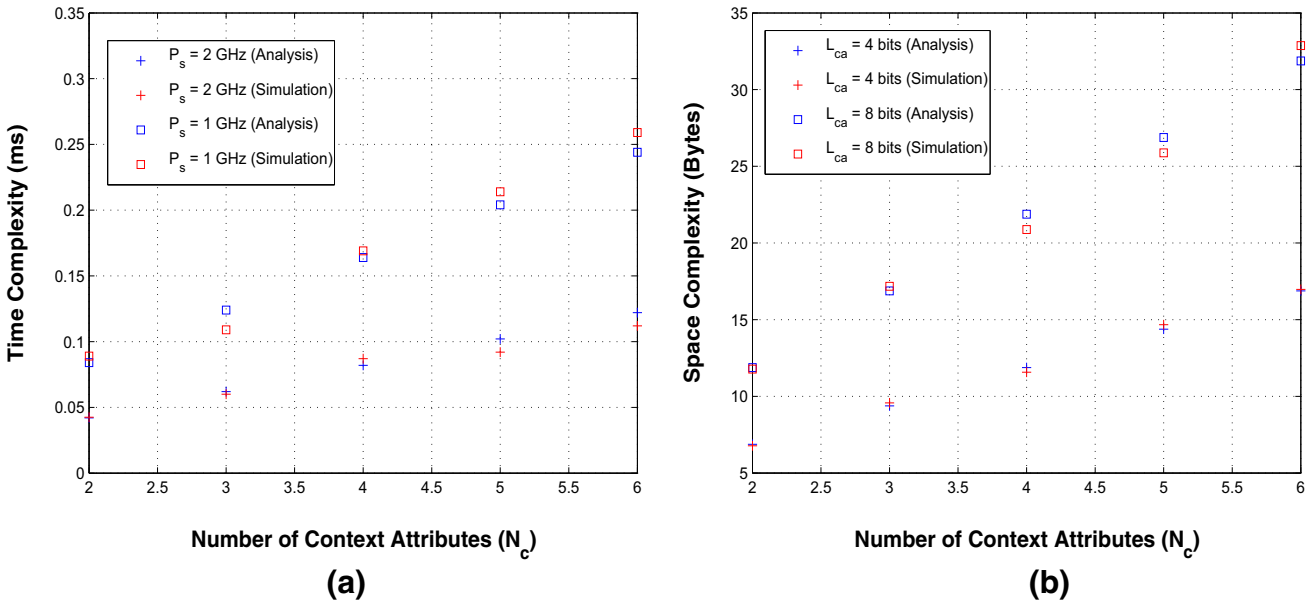

Fig. 3 Time and space complexity analysis (**a**, **b** vs total context attribute (N_c))

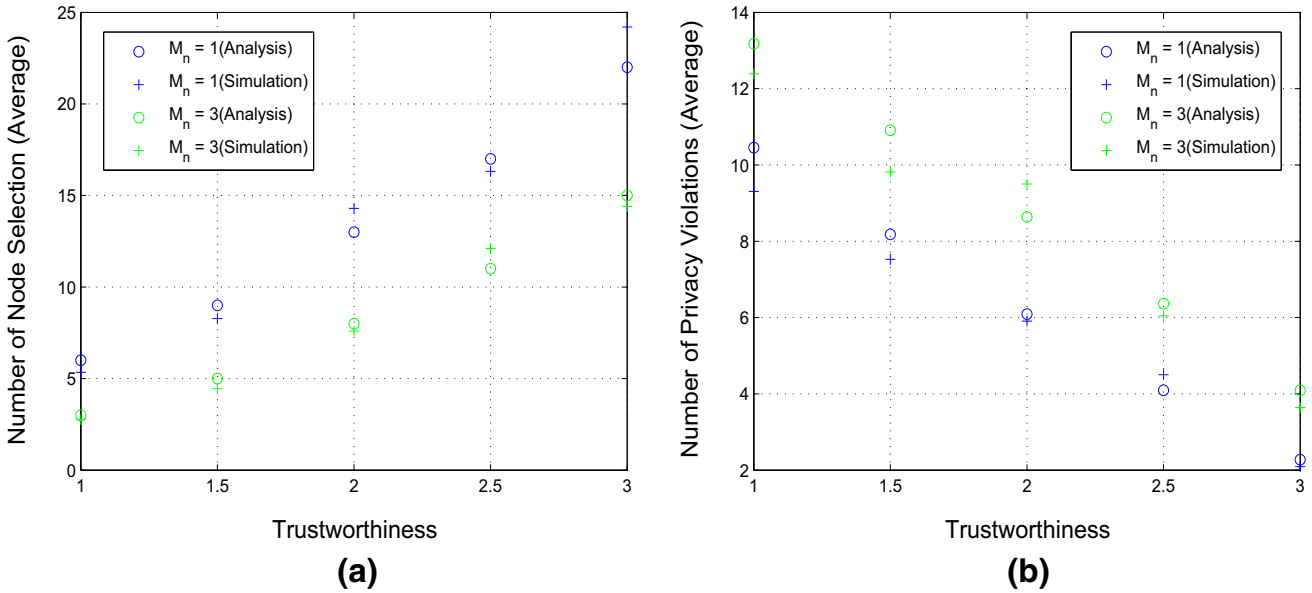

Fig. 4 Analysis and simulation of node's Behaviour. **a** Number of node selection. **b** Number of privacy violations

Eq. 16. Since, each privacy policy consists of N_c context attributes, the privacy policy stability index (SI_{pp}) is given by Eq. 17.

$$SI_{cap} = \frac{\sum_{j=1}^{k_n} m_{n,j} SI_{n,j}}{\sum_{j=1}^{k_n} m_{n,j}} \tag{16}$$

$$SI_{pp} = \frac{\sum_{j=1}^{N_c} SI_{cap}^{j}}{N_c} \tag{17}$$

6 Simulations and Results

In this Section, we provide the simulation environment, discuss the obtained analytical and simulation results, and evaluate the performance of proposed work by comparing with reactive protocols, AODV [33] and TARo [23]. We

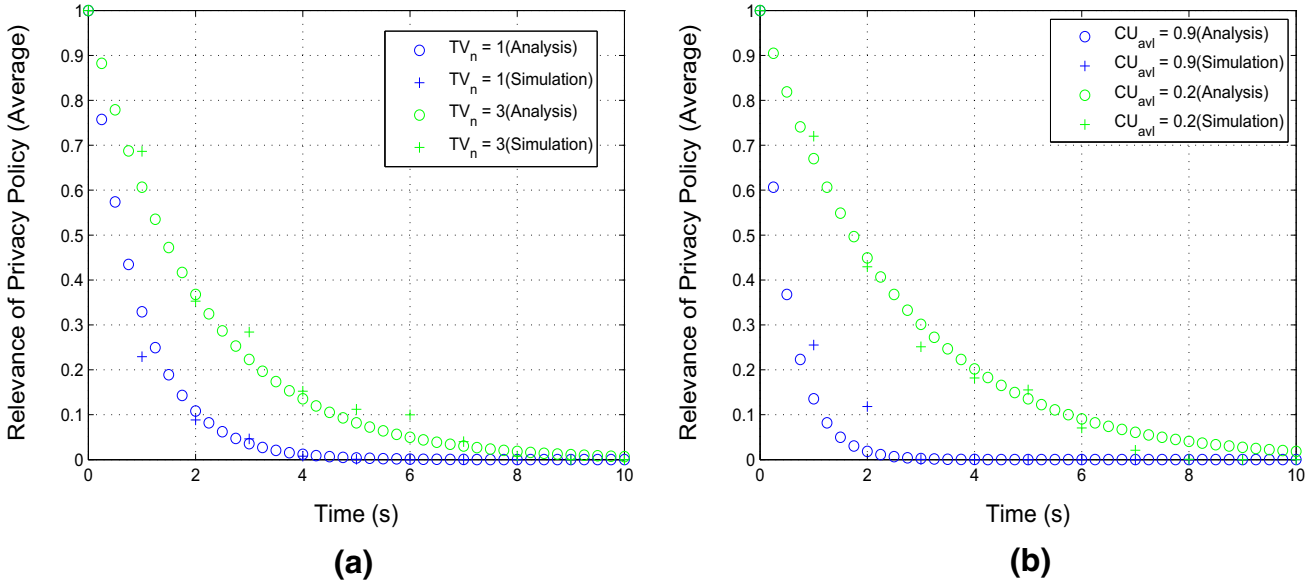

Fig. 5 Relevance of privacy policy. **a** Varying trustworthiness. **b** Varying uncertainty of context attribute parameter

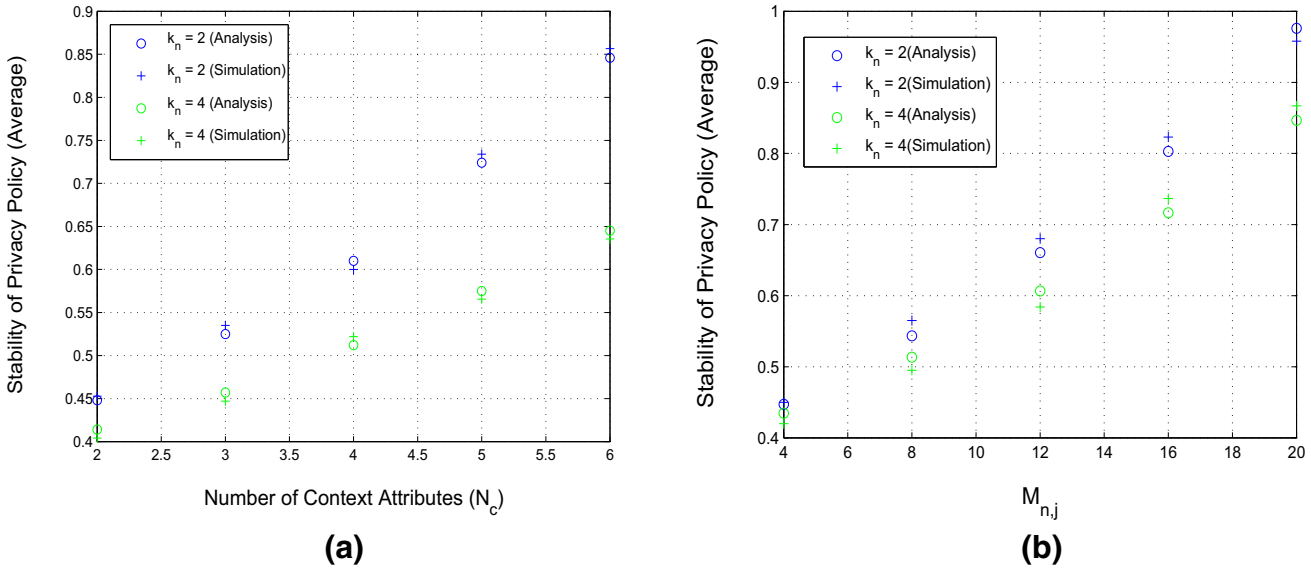

Fig. 6 Stability of privacy policy (vs total context attributes (N_c) **a**; vs number of objects ($M_{n,j}$) **b**)

choose reactive protocols as they are on-demand, and have low processing and computational overhead at a node.

6.1 Simulation Environment

The environment is simulated in network simulator (NS - 2.34 [34]) for testing the performance of privacy policies. We consider bidirectional wireless links with 20 Mbps capacity. Transmission range of all the nodes are same and have a constant value, and nodes move randomly with same mobility speed, whereas number of sender and receiver pairs (Se-Re pairs) is varied. Each simulation duration was set to be 500 s, and the final results were average of 100 simulations. Table 5 gives the details on simulation parameters.

6.2 Results and Discussion

We discuss the results obtained for the performance of privacy policies, and also compare the performance of proposed work with AODV [33] and TARo [23] in terms of routing efficiency.

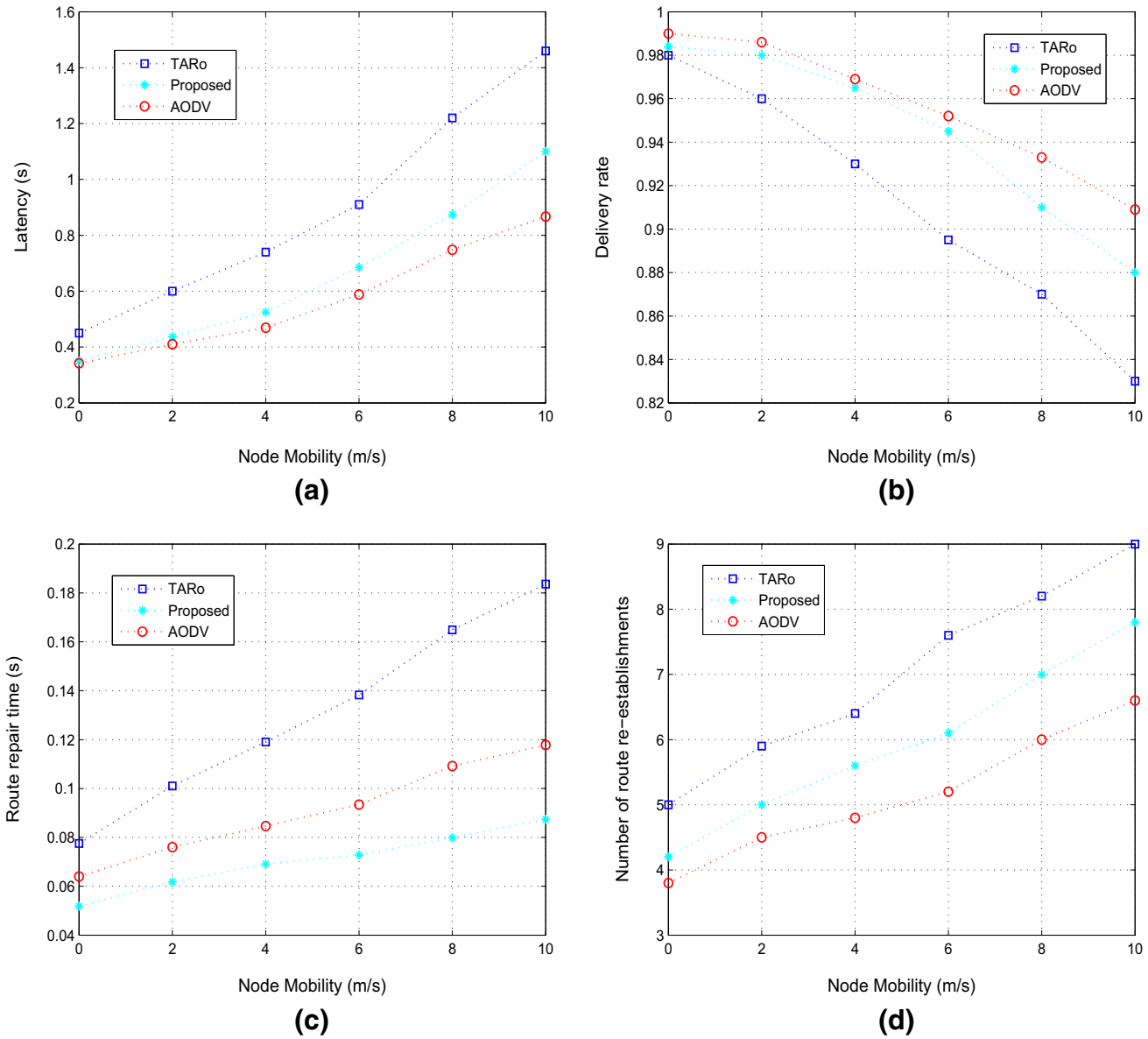

Fig. 7 Comparison of proposed work with AODV and TARo. **a** Latency. **b** Delivery rate. **c** Route repair time. **d** Number of route re-establishments

6.2.1 Complexity Analysis Results

For analyzing the complexity for designing privacy policies, γ is kept constant at 2 arrivals/sec, D_{dt} is considered to be 300 s, and t_{pf} is 0.001 s. Figure 3a, b, shows the analytical and simulation result for time and space complexity, respectively, with variation in N_c (in this case n_{dc} is kept constant at 2). From both the Figures, we observe that with the increase in N_c there is an increase in time and space complexity. We notice that the processing speed effects the time complexity, i.e., higher processing speed requires less time to design a privacy policy. Similarly, attributes with more length (L_{ca}) have high space complexity.

6.2.2 Results of Behavioural Analysis of Intermediate Nodes

To analyze the behaviour of trusted intermediate nodes, we consider nodes with varying trustworthiness and privacy maintenance level. Figure 4a, shows the number of times an intermediate node is selected for data transfer with variation in trustworthiness and privacy maintenance level, where we observe that the number of node selection increases with increase in node's trustworthiness, and node selections are higher for node with lower privacy maintenance level. Figure 4b, shows the number of privacy violations by intermediate node with variation in

trustworthiness and privacy maintenance level, where we observe that for the lower value of privacy maintenance level (i.e., node is reliable), number of privacy violations are low. Also, with increase in trustworthiness, the number of privacy violation are decreasing.

6.2.3 Results of Dependency Analysis on Context Attribute

Figure 5a, b, shows the relevance of privacy policies (wrt time) with varying source credibility (or trustworthiness, TV_n) and availability uncertainty of context attribute (CU_{avl}). For analysis, N_c is kept constant at 6, and f_c is varied between [0, 12] s. We observe that relevance of privacy policies decreases with time in both the Figures. In Figure 5a, CU_{avl} is kept constant at 0.6 and node's trustworthiness is varied, and we see that the relevance of privacy policy is high for the node with higher trustworthiness. In Fig. 5b, trustworthiness is kept constant at 2 and node's CU_{avl} is varied, and we see that relevance of privacy policy decreases at faster rate for higher CU_{avl} when compared to lower CU_{avl} values. Figure 6a, b, shows the stability of privacy policy with varying N_c and $M_{n,j}$ for $k_n = 2$ and 4. For Figure 6a, $M_{n,j}$ is kept constant at 4 and for Fig. 6b, N_c is kept constant at 2. We see that, there is increase in stability with increase in N_c and $M_{n,j}$. We also see that, there is a decrease in stability with increase in k_n, since, increase in k_n leads to small length categorization of context attribute value.

6.2.4 Results of Comparison with AODV and TARo

The following metrics are considered to evaluate the performance of proposed work in terms of routing efficiency: (1) Latency—time taken by a packet from a sender to a receiver; (2) Delivery rate—the portion of data packets which are delivered successfully to a receiver; (3) Route repair time—time required to repair a route by nodes en route; and (4). Number of route re-establishments—the number of route repairs by nodes en route.

In Fig. 7a, we see that the proposed work has similar latency when compared to AODV for lower node mobility. However, it increases slightly for higher node mobility. The proposed work achieves lower latency when compared to TARo. Figure 7b shows that the delivery rate of proposed work is slightly lower than AODV but much higher than TARo. The encryption of data at each hop introduces higher computations in the TARo which leads to increase in latency and decrease in delivery rate. Figure 7c shows the route repair time, where we see that the route repair time is lowest for the proposed work. It is because, in TARo a *rerr* message is sent back to the sender for route repair, however, in the proposed work route is locally repaired consuming less time. In Fig. 7d, we see that the number of route re-establishment for the proposed work is higher when compared to AODV, as the proposed work also considers route change due to privacy violations. Due to multiple routes in TARo, there are higher route failures, which results in higher route re-establishment.

7 Conclusions

The paper focuses on performance analysis of proposed privacy protection system during data transfer, where privacy policies are designed for trusted intermediate nodes by utilizing the application and context attributes. Analysis is discussed for *Complexity Analysis*, *Behavioural Analysis of Intermediate Nodes*, and *Dependency Analysis on Context Attribute*. The proposed work is compared with previous works using simulations. Results obtained show that the proposed work performs better. The model can be used in other privacy protection system by incorporating the details and functioning of the respective system. Future work aims at strengthening the performance analysis model by considering various factors. For example, spatial and temporal resolutions of context attribute to determine relevance of privacy policy.

References

1. J. Hoebeke, I. Moerman, B. Dhoedt and P. Demeester, An overview of mobile ad hoc networks: applications and challenges, *Journal of the Communications Network*, Vol. 3, pp. 60–66, 2004.
2. X. Hong, J. Kong, and M. Gerla. A new set of passive routing attacks in mobile ad hoc networks. pages 796–801, 2003.
3. H. Choi, P. McDaniel, and T. F. La Porta. Privacy preserving communication in manets. In *2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, pages 233–242, 2007.
4. Y. Yang, M. Shao, S. Zhu and G. Cao, Towards statistically strong source anonymity for sensor networks, *ACM Transactions on Sensor Networks (TOSN)*, Vol. 9, No. 3, pp. 1–23, 2013.
5. A. A. Bakar, A. A. Ghapar, and R. Ismail. Access control and privacy in manet emergency environment. In *Computer and Information Sciences (ICCOINS), 2014 International Conference on*, pages 1–6, 2014.
6. B. Shebaro, O. Oluwatimi and E. Bertino, Context-based access control systems for mobile devices, *IEEE Transactions on Dependable and Secure Computing*, Vol. 12, No. 2, pp. 150–163, 2015.
7. C.-J. Y Chiang, S. Demers, P. Gopalakrishnan, L. Kant, A. Poylisher, Y.-H. Cheng, R. Chadha, G. Levin, S. Li, Y. Ling, S. Newman, L. LaVergne, and R. Lo. Performance analysis of drama: A distributed policy-based system for manet management. In *Proceedings of the 2006 IEEE Conference on Military Communications*, MILCOM'06, pages 272–279, 2006.
8. R. Zheng, J. Hou and L. Sha, Performance analysis of power management policies in wireless networks, *IEEE Transaction on Wireless Communications*, Vol. 5, pp. 1351–1361, 2006.

9. V. S. Soares, F. F. Farahmand and J. R. Rodrigues, Performance analysis of scheduling and dropping policies in vehicular delay-tolerant networks, *International Journal on Advances in Internet Technology*, Vol. 3, No. 1, pp. 137–145, 2010.
10. G. R. Gupta and N. B. Shroff, Delay analysis and optimality of scheduling policies for multihop wireless networks, *IEEE/ACM Transactions on Networking*, Vol. 19, No. 1, pp. 129–141, 2011.
11. J. Zheng, J. Dong Li, Q. Liu, H. Shi, and X. Niu Yang, Performance analysis of three multi-radio access control policies in heterogeneous wireless networks, Science China Information Sciences, Vol. 56, No. 12, pp. 1–10, 2013.
12. K. Fisler, S. Krishnamurthi, L. A. Meyerovich, and M. Carl Tschantz. Verification and change-impact analysis of access-control policies. In *Proceedings of the 27th International Conference on Software Engineering*, ICSE '05, pages 196–205, 2005.
13. L. Duan, Y. Zhang, S. Chen, X. Liu, B. Cheng, and J. Chen. Model-based minimum privacy disclosure recommendation for authorization policies. In *2016 IEEE International Conference on Services Computing (SCC)*, pages 403–410, 2016.
14. W. Apolinarski, M. Handte, and P. J. Marrn. Automating the generation of privacy policies for context-sharing applications. In *Intelligent Environments (IE), 2015 International Conference on*, pages 73–80, 2015.
15. S. Talib, S. M. Abdul Razak, A. Olowolayemo, M. Salependi, N. F. Ahmad, S. Kunhamoo, and S. K. Bani. Perception analysis of social networks' privacy policy: Instagram as a case study. In *Information and Communication Technology for The Muslim World (ICT4M), 2014 The 5th International Conference on*, pages 1–5, 2014.
16. M. Guarnieri, M. Arrigoni Neri, E. Magri, and S. Mutti. On the notion of redundancy in access control policies. In *Proceedings of the 18th ACM Symposium on Access Control Models and Technologies*, SACMAT '13, pages 161–172, 2013.
17. P. Rao, D. Lin, E. Bertino, N. Li, and J. Lobo. Exam: An environment for access control policy analysis and management. *IEEE Workshop on Policies for Distributed Systems and Networks*, pages 238–240, 2008.
18. J. Lobo, E. Bertino, P. Rao, R. Ferrini and D. Lin, A similarity measure for comparing xacml policies, *IEEE Transactions on Knowledge & Data Engineering*, Vol. 25, No. 9, pp. 1946–1959, 2013.
19. E. Bertino, C. Brodie, S. B. Calo, L. F. Cranor, C. Karat, J. Karat, N. Li, D. Lin, J. Lobo, Q. Ni, P. R. Rao and X. Wang, Analysis of privacy and security policies, *IBM Journal of Research and Development*, Vol. 53, No. 2, pp. 1–18, 2009.
20. H. Hongxin, G.-J. Ahn and K. Kulkarni, Discovery and resolution of anomalies in web access control policies, *IEEE Transactions on Dependable and Secure Computing*, Vol. 10, No. 6, pp. 341–354, 2013.
21. A. A. Bakar and E. H. E. El-Talib, Android mobile application for privacy data access in manet emergency services, *Information Science and Applications (ICISA)*, Vol. 2016, pp. 623–631, 2016.
22. H. J. H. Aldabbas, T. Alwada'n, and A. Al-Bayatti, Data confidentiality in mobile adhoc networks, *International Journal of Wireless and Mobile Networks (IJWMN)*, Vol. 4, pp. 225–236, 2012.
23. J. Chen, R. Boreli, and V. Sivaraman. Taro: Trusted anonymous routing for manets. In *2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, pages 756–762, 2010.
24. A. J. Aviv, M. Sherr, M. Blaze, and J. M. Smith. Privacy-aware message exchanges for geographically routed human movement networks. In *17th European Symposium on Research in Computer Security*, pages 181–198, 2012.
25. B. Miller, K. Buck, and J. D. Tygar. Systematic analysis and evaluation of web privacy policies and implementations. In *Internet Technology And Secured Transactions, 2012 International Conference for*, pages 534–540, 2012.
26. W. Li, A. Joshi and T. Finin, Cast: Context-aware security and trust framework for mobile ad-hoc networks using policies, *Distributed and Parallel Databases*, Vol. 31, No. 2, pp. 353–376, 2013.
27. C. Camara, P. Peris-Lopez and J. E. Tapiador, Security and privacy issues in implantable medical devices: A comprehensive survey, *Journal of Biomedical Informatics*, Vol. 55, pp. 272–289, 2015.
28. W. Wang and T. Stransky, Stateless key distribution for secure intra and inter-group multicast in mobile wireless network, *Computer Networks*, Vol. 51, No. 15, pp. 4303–4321, 2007.
29. B. S. Bhati and P. Venkataram, Performance analysis of location privacy preserving scheme for manets, *International Journal of Network Security*, Vol. 18, pp. 736–749, 2016.
30. Z. Pawlak. Rough sets. In *International Journal of Computer and Information Sciences*, Vol. 11, No. 5, pp. 341–356, 1982.
31. T. D. S. Keerthi and P. Venkataram. Aodv route maintenance using honeypots in manets. In *2015 World Congress on Internet Security (WorldCIS)*, pages 105–112, 2015.
32. M. J. Beynon, Stability of continuous value discretisation: an application within rough set theory, *International Journal of Approximate Reasoning*, Vol. 35, No. 1, pp. 29–53, 2004.
33. C. Perkins, E. Belding-Royer, and S. Das. Ad hoc on-demand distance vector (aodv) routing. In *RFC 3561*, 2003.
34. The network simulator ns-2.34 available at: http://www.isi.edu/nsnam/ns/.

Bhawani Shanker Bhati received his Bachelor of Engineering (B.E.) degree from the CMR Institute of technology, Bangalore, India, in 2009, and Master of Engineering (M.E.) degree from the Indian Institute of Science, Bangalore, India, in 2012. He is currently pursuing his Ph.D. in Indian Institute of Science, Bangalore, India. His research interests are in the areas of wireless and adhoc communication, communication protocols, ubiquitous computing and privacy in wireless networks.

Pallapa Venkataram received his Ph.D. Degree in Information Sciences from the University of Sheffield, England, in 1986. He is Professor in the Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore, India. Dr. Pallapa's research interests are in the areas of Wireless Ubiquitous Networks, Communication Protocols, Computation Intelligence applications in Communication Networks and Multimedia Systems. Dr. Pallapa is the holder of a Distinguished Visitor Diploma from the Orrego University, Trujillo, PERU. He has published over 200 papers in International/national Journals/conferences. He has received best paper awards at GLOBECOM'93 and INM'95 and also CDIL (Communication Devices India Ltd) for a paper published in IETE Journal. He is a Fellow of IEE (England), Fellow of IETE (India) and a senior member of IEEE Computer Society.