International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 2, April 2020, pp. 1561~1569
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i2.pp1561-1569

Trust correlation of mobile agent nodes with a regular node in a Adhoc network using decision-making strategy

Chethan B. K.[1], M. Siddappa[2], Jayanna H. S.[3]
[1]Department of Information Secience and Engineering, Sri Siddhartha Institute of Technology, India
[2]Department of Computer Science and Engineering, Sri Siddhartha Institute of Technology, India
[3]Department of Information Secience and Engineering, Siddaganga Institute of Technology, India

Article Info

Article history:

Received Mei 28, 2019
Revised Sep 17, 2019
Accepted Sep 27, 2019

Keywords:

Attack
Mobile adhoc network
Mobile agent
Probability
Security

ABSTRACT

A mobile agent offers discrete advantage both in facilitating better transmission as well as controlling the traffic load in Mobile Adhoc Network (MANET). Hence, such forms of network offers maximized dependencies on mobile agents in terms of its trust worthiness. At present, there are various work being carried out towards resisting security breach in MANET; however approaches using mobile agent based mechanism is few to found. Therefore, the proposed system introduces a novel mathematical model where an extensive decision making system has been constructed for identifying the malicious intention of mobile agents in case they go rogues. By adopting multi-tier communication policy and fairness concept, the proposed system offers the capability to resist any form of malicious activity of mobile agent without even presence of any apriori information of adversary. The outcome shows proposed system outshines existing security scheme in MANET.

Copyright © 2020 Institute of Advanced Engineering and Science.
All rights reserved.

Corresponding Author:

Chethan B. K.,
Department of Information Secience and Engineering,
Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India.
Email: crsh2019@gmail.com

1. INTRODUCTION

The mobile Adhoc network (MANET) is distributed network of moving nodes without having any access point in its deployment, where the participating nodes collaborate itself to the neighbour nodes whose physical distance is lower than the communication ranges of the nodes [1]. In the post PC-era, various independent or a sub-system of Internet of Things (IoT) based applications requires a infrastructure less wireless network, where MANET plays an important role [2]. The MANET working group, many academician and industrial researchers contributed to evolve many proactive and reactive routing protocols to makes the success of the network performance in terms of the data delivery and achieve any source to any destination kind of the communication [3-5].

Since MANET is a resource constraints network of mobile nodes with limited power as operated by battery and bandwidth, a non-optimal or un-balance usages of these resources drastically reduces the network performance as well the resource utilization is exponential to the number of nodes, as O (n2) that makes its limited uses where scalability is in demand [6]. The various such issues like scalability and associated congestion problem, link failures due to obstacles etc, the concept of self-configurable mobile agent is used [7-11]. Though there are enormous benefits of adopting additional nodes in a MANET as a mobile agent which can facilitates large scale routing and ensure to enhance the network performance but since many of the attacks takes place in the MANET are by introducing malicious nodes by exploiting the vulnerabilities due to of the self-configuration characteristics [12].

It is an open research issues to find the reliability in terms of trust by the regular MANET nodes with the mobile-agent nodes, which ensures the degree of security to establish route in the MANET with mobile-agent nodes. The initial approaches for finding the node trust level were adopted at the local layer of the nodes that limits the auditing accuracy and capacity to identify the types of attacks [13]. The further evolution in the direction of the node trust determination, the methods uses the local level capacity along with cooperative mechanisms to detect the various kinds of the attacks, but these approaches poses additional overhead as many control messages are required to be imposed to exchanges the updated information at both local level as well as in collaborative communication that leads it to work in a cluster [14-15]. The methodologies for the security aspects in terms of identifying the malicious nodes implanted or participated into the MANET is given to a particular node in a cluster that minimizes overheads to an extend but due to distributed and highly dynamic nature of the network it poses again polynomial complexities when it is a large-scale network.

The approach of additional methods like signature, anomaly engine etc were developed to mark a suspicious node as malicious and avoid it from the routing but it makes the iterative network partition which is not a perfect solution to balance the requirement of the balance between the security and the network performance [16]. Thus, inspite of a control mechanism for the attacks and threats due to malicious node a method of mitigating the effect is adopted based on the strategic decision made by the nodes and the mobile agents that ensure a balance between the minimization of loss due to security threats and maximization of the network performance QoS parameters balancing both resources even in the large network which a demand of the future applications. This paper presents a mathematical model of a decision-making strategy among the regular-manet nodes and the mobile-agent nodes to establish a trust for the reliable communications. The organization of the proposed manuscript is as follows: Section 1 discusses about the background of the existing studies associated with agent based solution toward security, security briefs of research problems identified and highlights about the research methodology adopted for solving the problems of existing security issues in MANET. Section 2 presents an illustrative discussion of system design followed by discussion of the result analysis in Section 3. Finally, the conlusion of the proposed system is briefed in Section 4.

There is absolutely no doubt of presence of archives of massive literature highlighting about the techniques required for securing the MANET system. The most recent study carried out by Wang and Li [17] have presented a secure communication mechanism that selects the agent nodes which contructing routes. These techniques ensure reliable delivery of packet between the agent nodes. Another recent work of Shehada et al. [18] has adopted trust based scheme along with reputation in order to model a mobile agent focusing on social network. The technique uses an adaptive process in order to evolve up with a decision makig system. Agent-based approaches are also used by Harrabi et al. [19] where the authors have used it over vehicular network. The work carried out by Rohankar [20] throws an interesting usage of agent-based approach over wireless adhoc network using predictive approachover conventional MANET routing scheme. However, the approach was more focus on communication establishment and less focus on security. Study considering securing adhoc network using mobile agents was seen in the work of Abosamra et al. [21] where authors have used encryption protocol for securing the communication. Combination of agent usage and trust is another frequently adopted approach for securing communication in MANET.

The work of Halim et al. [22] has introduced a selective data forwarding scheme using mathematical model using the role of agent for both routing and monitoring system considering on-demand routing scheme. The study outcome shows better performance in latency and detection. The agent-based mechanism was also used in IoT and cloud ecosystem as MANET finds its ultimate deployment over this. The recent works carried out by Magarino et al. [23] have used agent-based approach for facilitating mining massive data. Another recent work of Fortino et al. [24] has discussed how agent-based mechanism can be embedded with smart objects in IoT environment. The work of Gargees and Scott [25] has presented a technique for facilitating data structurization over IoT media in order to extract pattern of communication. However, such studies are more data oriented and less on security.

Adoption of multi-agents was reported to be used in the study carried out by Quan et al. [26, 27] which emphasizes on both fault tolerance and security breach prevention. Another work carried out by Fortino et al. [28] have discussed that hybridizing the charecteristics of agents has multiple benefits of communication system assessment in an IoT. The study carried out by Santos et al. [29] have discussed about the usage of softwarer agents along with incorporation of intelligence. The work carried out by Hsieh et al. [30] have constructed a design of an agent that using event-driven approach for constructing the communication mechanism in IoT. Therefore, there are various mechanisms evident in existing approach where agent-based approach has been utilized. However, there is less inclination of the existing schemes to address security problems associated with MANET and are more focus on re-defining communication system on wireless network. The next section briefs of research problems.

The significant research problems are as follows:

- None of the existing agent-based scheme has addressed the complex security problems in MANET or likewise scenario.
- The adversaries are well defined in existing security schemes that uses mobile agents and hence they are not applicable if the adversary tactics changes.
- Developing intrusion detection system using mobile agent in presence of dynamic adversary is not much emphasized in existing system.
- There are no benchmarked studies focusing on solving the critical security problems in case the mobile agents are compromised.

Therefore, the problem statement of the proposed study can be stated as "*It is quite a challenging task to construct a framework capable of identifying the discrete behaviour of mobile agents such that agent-based communication system can be further boosted for MANET communication*"

The proposed system is implemented using analytical research methodology where the prime focus is offered towards constructing a secured scheme to offer selection of trusted mobile agents in MANET. Basically, mobile agents assist in multiple ways to bridge the communication demands in MANET but are highly vulnerable to security threats. Therefore, proposed system considers a presence of adversarial model where there is no apriori information about the criticality of attack in MANET by malicious mobile agents. The scheme adopted as a solution is showcased in Figure 1

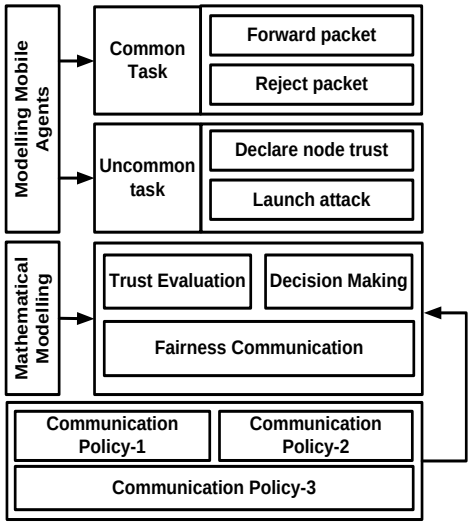

Figure 1. Schema of methodology for 1st objective

The above Figure.1 exhibits that the proposed system considers modeling mobile agents with inclusion of two types of task to be executed by them. Owing to presence of common task, it is highly challenging to distinguish regular node from malicious mobile agent. Although, there are distinct charecteristics too, but they are rarely expected to be exhibited by malicious mobile agent in order to resist the chances to get entrapped by the security system.Therefore, the proposed model constructs a simplified mathematical modeling on the basis of probability theory in order to evolve up in a potential and reliable decision making system. The core components of the proposed mathematical modeling are trust evaluation, decision making, and fairness communication. A novel concept of trio communication policy has been constructed which governs all the possibilities of communication behaviour of both the type of nodes. The next section illustrates about the system design and implementation.

2. SYSTEM IMPLEMENTATION

The complete target of the system design is to construct a mechanism that offers enhanced capability to identify the malicious intention of mobile agent. The outcome of the implementation is mainly focused on quarantining such adversary node to participate in communication process. The backbone concept of system implementation is to construct a reliable intrusion detection system mainlyover MANET. These section briefs of complete information associated with the system implementation.

2.1. Modelling assumptions

The *primary* assumption of the proposed system is that there is no apriori information associated with the identity of the adversary node. This assumption will offer evidence of resistivity capability of regular node against malicious node. The *secondary* assumption of the proposed system is that adversary will always target mobile agents as their initial source of launching attack. The rationae behind this assumption is that network resource used for compromising a regular node is more than that of mobile agent. If one mobile agent is compromised than the attack will spread exponentially because one mobile agent assists in communication for multiple neighboring nodes. The *tertiary* assumption is that there are possibilities of slight variation in observation for adversarial mobile agent; however, study considers such probability to be very low. This justification behind this assumption is that the proposed system performs intrusion detection system on the basis of monitoring of neighboring mobile agents. Owing to inclusion of dynamic topology in MANET, there are some possibilities that a good malicious node could be declared as adversary or vice-versa. This challenge is addressed by using a threshold-based evaluation system which reduces such chances.

2.2. Mathematical model

Probability-based modeling has been used for construction the mathematical framework of proposed system for assessing the trust factor from the mobile agents. The proposed study considers that there are two kinds of mobile agents i.e. regular mobile agent and malicious mobile agent. An adversarial modeling is carried out by considering *correlated trust parameter* and *uncorrelated trust parameters* represented as,

$$\lambda_{ct}=\{F_p, R_j\} \ \& \ \lambda_{uct}=\{C_n, D_{nt}\} \quad (1)$$

The correlated trust parameter λ_{ct} will mean a set of certain task executed by mobile agents, which are found correlated in both regular and adversary mobile agents. The study considers F_p (forward packet) and R_j (reject packet) which can be carried out by both regular and adversary mobile agent, which makes it hard to distinguish them in intrusion detection system. The uncorrelated trust parameter λ_{uct} will mean certain distinct task explicit to node type viz. i) the proposed study consider C_n (compromize / launch malicious code) to be executed by adversary only while D_{nt} (declare node trust) is explicitely a task carried out by regular mobile agent. These operations can only distinguise if the mobile agent is malicious or non-harmful. The essential components of the proposed mathematical modeling are as follows:

- **Trust Evaluation**: The proposed system performs three types of trust evaluation in order to ascertain the trust worthiness of the communicating mobile agent using two parameters viz. i) Q_1(computing frequencies of F_p) and ii) Q_2 (computing frequencies of R_j). The *first* trust evaluation factor T_R is termed as *regular trust* and is computed as $Q_1/(Q_1+Q_2)$ while the second trust evaluation factor T_M is termed as *malicious trust* and is computed as $Q_2/(Q_1+Q_2)$. The *third* trust evaluation T_{am} is termed as *ambiguous trust* and is computed as following:

  $$T_{am}=c.\ \tau_1/\tau_2 \quad (2)$$

  In the above mathematical expression, the variable *c* is network constant while the variable τ_1 is scalar product of T_R and T_M. The variable τ_2 is computed as scalar squared product and summation of Q_1 and Q_2 respectively.
- **Decision Making**: In order to make a decision, it is essential for the proposed system to observe the trend of communication for all the mobile agents. For this purpose, the proposed system considers little more parametric computation associated with profit and number of resources being used by mobile agents. This behavioural trend will offer more inclusive disclosure of their malicious intention. The initial decision making towards capturing malicious intention of mobile agent will be seen from the trend of ambiguous trust T_{am} values (2). Normally, a declining trend of numerical value of ambiguous trust T_{am} will show concrete case of adversary while a regular node will never be shown to be has declining trend owing to the usage of cut-off *Thr* which can be given as per the demand of security. Apart from this, a second layer of cut-off is used in order to prevnt any possibility of outliers in declaration of regular mobile agent to malicious one.
- **Fairness Communication**: As the proposed system is designed on the basis of neighboring mobile agent behavioural monitoring system, there are chances that certain numerical evaluation could lead to wrong misinterpretation of mobile agents to be malicious. This situation is avoided in following manner. The proposed system develops a concept of fairness to both malicious and regular mobile agent in order to ensure that the system can still identify the malicious behaviour in case of ambiguous decision making. According to this fairness concept, the regular mobile agent is considered to more inclination towards identifying and updating the threat (i.e. D_{nt}) whereas the malicious node will be more inclined towards

launching malicious codes to the neighboring mobile nodes in MANET. This situation makes the communication more challenging as both the agent types will try to gain more fairness. This situation is solved by following when the regular mobile agent evaluates the trust of neighboring mobile agents; it reconfirms the malicious intention by checking the trust value of the target mobile agent from its neighboring nodes. That trust is then compared with the second layer of trust cut-off to finally declare the target node to be malicious.

2.3. Execution flow

The proposed system initiates with the configuraton of deployment region *D*, number of mobile agents *n*, and proportion of the intruder node i_{node}. Apart from this variable, the proposed system also performs initialization of few more parameters e.g. $P(F_p)$ profit allocated to agent for performing F_p, $\gamma(F_P)$ number of resourced involved in performing F_P, $P(C_n)$ profit allocated to agent for performing C_n. The next part of the implementation is carried out for estimating Q_1, Q_2, p_a, and T_{am} for all the mobile agents present in deployment region *D*. The proposed system implements three different communication policies as a part of contribution for assisting in better decision making as well as mapping with real-world greedy scenario of the mobile agents. The three communication policies are as follows:

- *Communication Policy-1 (CP1)*: According to this policy, the current mobile agents will have complete information about the next task to be executed by the mobile agent and vice-versa.
- *Communication Policy-2 (CP2)*: In this policy, a probability is assigned to each undertaking of CP1 thereby allowing the mobile agents to arbitrarily opt for CP1. As there are infinite number between the probability limits so there is massive number of combination of CP1 for each mobile agent.
- *Communication Policy-3 (CP3)*: In this policy, the current mobile agents don't have complete or has fuzzy information about the communication policy of target mobile agents. One interesting fact of this communication policy is that tactic adopted by the mobile agent gives indication about the trust factor on the basis of historical information.

All the above communication policies are constructed on the basis of various tasks i.e. F_P, C_n, R_J, and D_{nt}. The proposed system is then assessed on the basis of combination of all three communication policies adopted by regular and malicious mobile agents. The assessment is carried out by selecting a source mobile agent and destination node. This principle is used for identification of the malicious mobile agents whose algorithmic steps is shown as below:

Algorithm for Identification of Malicious Agent

Input: n, ψ, *Thr*, p_a
Output: *F*
Start
1. **For** i=1:n
2. **While** ψ<Thr
3. **If** p_a<$cond_1$ **then**
4. opt $F_p(prob_1)$
5. **Else**
6. opt $F_p(prob_2)$
7. **End**
8. **End**
9. *F*→flag vulnerable mobile agent
10. **End**
End

The above algorithm takes the input of n (total number of mobile agents), ψ (selected trust), Thr (cut-off trust), and p_a (probability of adversary node) that after processing yields and outcome of F (Declaring Adversary Node). According to the above mentioned algorithm, the computation towards the identification of the malicious agents is carriedout considering all the agents *n* (Line-1). The complete algorithm considers CP3 as the tactic adopted for mobile agent of unknown trust nature (which is under observation). Under this scheme, the source mobile agent performs evaluation of the target mobile agents in order to conclude if they the regular or malicious mobile agents. This evaluation is carried out by a variable *ψ* representing probability of vulnerable mobile agents and is computed by scalar product of probability of adversary node p_a and $(1-T_{am})$, where the later variable represents residual trust ambiguity (Line-2). It will therefore mean that if the variable ψ is found more than cut-off *Thr* than it will just mean that the target node doesn't have malicious intention. However, it still doesn't give a confirmation that the target node is 100% regular mobile agent. For this purpose, it performs further assessment.

The system compares probability of adversary node p_a with conditional parameter $cond_1$. The computation of the conditional parameter is carried out by using probability where the variable $cond_1$ represents *favorable chances of data forwarding by target mobile agent* divided by *total chances of both data forwarding and launching attack*. The estimation of first parameter is carried out by $P(F_P)$-$\gamma(F_P)$ while the later parameter is estimated as $P(F_P)+P(C_n)$. A closer look into the formation of the variable $cond_1$ will show that it represents the best chances of data forwarding by the mobile agent in present of all the probabilities connected with both data forwarding and launching attack. Therefore, the conditional statement in Line-2 represents that probability that the target mobile agent is an adversary and that is found less than conditional parameter $cond_1$. In such positive case, it will mean that the target mobile node could be malicious but it doesn't have any harmful action to be launched at that time.

Hence, there are good chances that target mobile node will perform data packet forwarding with higher probability $prob_1$ (Line-4). However, if the condition found to be P_a greater than it will mean that there are some good chances to confirm that the target node has malicious intention which can be calculated by different probability i.e. $prob_2$(Line-6). The value of $prob_1$ is 1 as it is higher probability score while the second probability $prob_2$ is estimated as favorable chances of attack ($\gamma(C_n)$- $\gamma(F_P)$) divided by total attack chances ($P(C_n)$). Finally, the system retains the latest value of Q_1, Q_2, and p_a and transmits to all neighboring mobile agents about the conclusion it draws from evaluation of target mobile agent in terms of flag message *F* (Line-9). Therefore, the proposed algorithm allows the source mobile agents / nodes in MANET to make use of probability on the basis of few operational parameters (Q_1, Q_2, and p_a) to estimate the malicious intention of the target mobile agent. The strength of this algorithm is that it offers multi-tier checks for the trust factor associated with the target mobile agents where trust score is extracted directly as well as from the neighboring nodes of the target mobile agents. Another interesting part of this algorithm is that even if the target mobile agent is not 100% confirmed tobe malicious, but if itscurrent intention is just to forward data packet than it is permitted to do so.

The logic behind this operation is that – a malicious node will try to bypass all security system in MANET as the network is highly dynamic order and chances of using distributed security protocols are usually high. Therefore, in order to resist disclosure of the malicious intention of an adversary they will act as a friendly node by participating as relay or intermediate mobile agents. An adversary will continue to do this until and unless they get an appropriate opportunity to launch malicious codes. Another interesting point of this algorithm is its incorporation of the fairness concept for both regular and malicious mobile agents. Usually, a malicious mobile agent will continue forwarding the packet as that is not their main intention; however, they will need to do so for not getting themselves catured by the security system. As it will require consumption of resources which is actually destined for launching an attack, so a threshold value can be selected for this. For an example, a malicious node cannot use 50% of their resources just to do F_P operation as they also require retaining resources for C_n operation. This concept is used in proposed system which can identify malicious mobile agent to a large extent. However, if their action is found to be within a tolerable cut-off of threshold, it will eventually mean that probability of launching attack is less by the malicious node and there is no harm allowing them in data packet forwarding.

Adopting this mechanism, all the target node is under consistent observation. Apart from this, there is also possibility about the wrong judgement about the legitimacy of the target mobile agent in communication region. For this purpose, the proposed system should first check if the anticipated value of the D_{nt} is found to be more than maximum score of probability of F_P and C_n. In such condition, it will mean that there are partial changes of outliers too. This problem is solved by assesing the variability of the probability score. A penalty factor is allocated in case of violation of the fairness factor by the regular malicious agent. Hence, irrespective of slight chances that some target nodes by misjudged, but in majority of cases the judgement is correct as the trust computation is carried out considering local and global trust factor. One of the interesting effectiveness of this security protocol is that it drains out the resources of the malicious nodes as neither it allows to participate in routing process (as long as their probability of launching attack is not found defined under existing communication policy) nor it allows to launch an attack. Hence, the proposed system offers a significant cost control by avoiding usage of any comlex encryption algorithm in order to resist any possibilities of intrusion.

3. RESULT ANALYSIS

The scripting of the proposed security scheme has been carried out over MATLAB. The analysis considers that is maximum loss could occur to a regular node if they generate falsified report. Therefore the cut-off value of the trust could be considered to be somewhat ideally between 0.4-0.5 and simulation area considered is $1000x1200m^2$. The assessment of proposed study was carried out by comparing its performance

with existing security scheme e.g. SAODV [31] and SLSP [32] with respect to multiple performance parameters e.g. latency, overhead, throughput, and processing time.

Figure 2 highlights the graphical outcome of comparative analysis that shows proposed system offers better performance in every aspect in comparison to existing system. The prime reason behind this are existing security schemes offers protection by assuming that the adversary is well known and all its actions are very much well defined. This is highly unpractical scenario and MANET when integrated with IoT can invoke adversary with exponentially high dynamicity. On the other hand, proposed system is capable to identify the malicious intention without even knowing exact specification of the adversary. The complete simulation is carried out considering that specific number of mobile agents where a both good and rogue agent exists in number but not in terms of identity. Hence, the proposed scheme supports faster updating process resulting in lower latency as shown in Figure 2 (a) and faster processing time Figure 2 (d).

Apart from this, owing to the adoption of the fairness concept, it was seen that proposed system even exploits malicious nodes if they make themselves available for data forwarding. Therefore, a higher controllable environment is developed which ensures that malicious mobile agent doesn't invoke attack and permits them to forward a data packet, This is also a good prevention approach as malicious node will soon drain out of energy which was primarlity destined for launching attack. This causes non-significant effect on the throughput resulting in a good balance between the security enhancement and data communication performance as shown in Figure 2(c). Apart from this the updating of the trust factor of the regular or malicious node is carried out only for the communicating nodes and neighboring nodes. This causes highly reduced overhead effect on the communication in MANET system. Therefore, the proposed system can be claimed of offering simplified solution towards upgrading security features for evaluating trust for mobile agents in MANET.

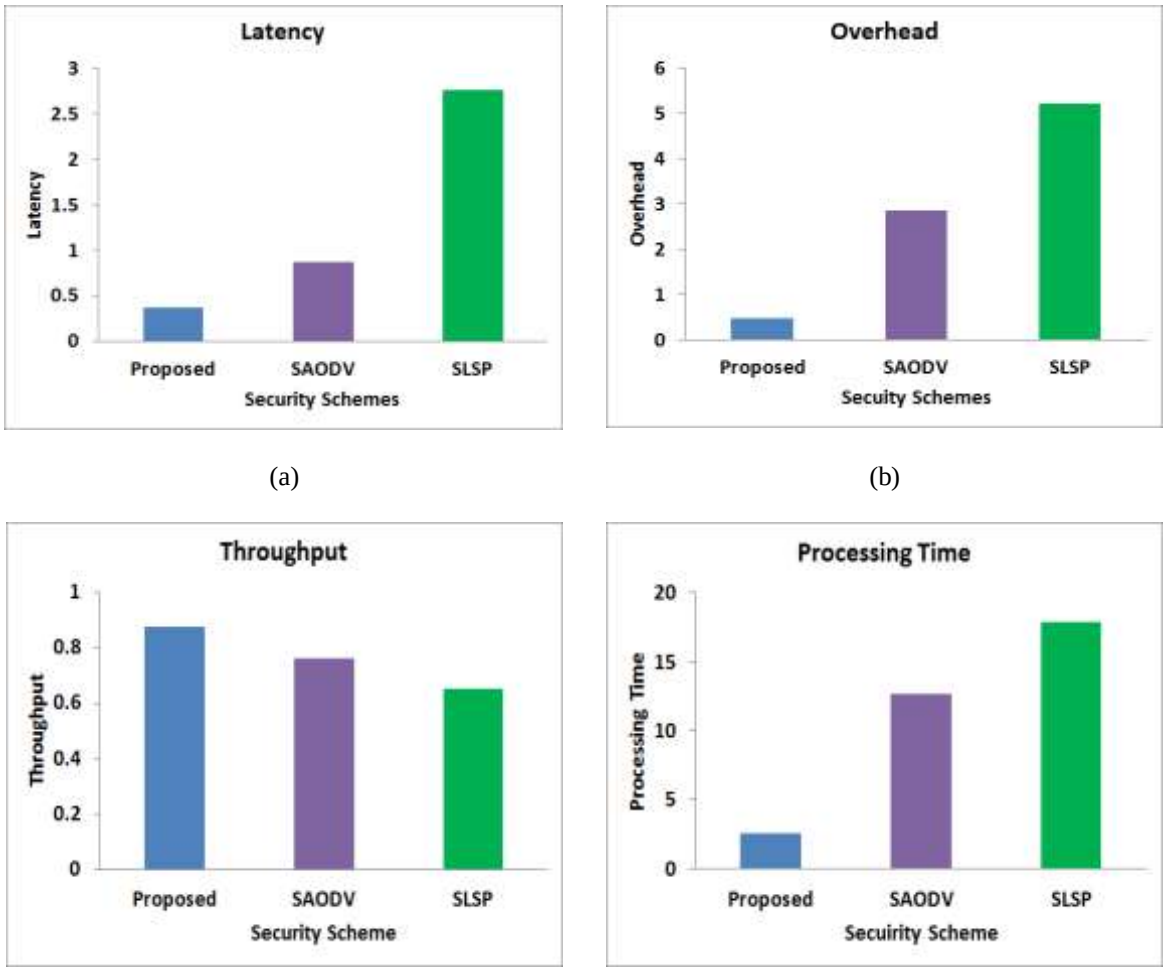

Figure 2. Comparative performance analysis, (a) Latency, (b) Overhead, (c) Throughput, (d) Processing time

4. CONCLUSION

Presence of a mobile agent in a dynamic network like MANET could offer an immese boost up in the communication process as they acts as a communication bridge between two communicating nodes. It will eventually mean that compromising mobile agents can break loose exponentially higher degree of vulnerability in the entire network. Therefore this challenging scenario cannot be dealt using existing mechanism which is highly application specific as well as attack-specific solution. Therefore, the proposed system offers discussion of a framework that uses probabilistic model for defining probable behaviour of communication of both regular node and malicious mobile agents in order to discretely identify them. The significant contribution of the proposed model are i) zero dependency on iterative based cryptographic protocols in MANET, ii) cost effective solution towards security without aprioi information about the attacks, and iii) it does balance the communication demands of MANET.

REFERENCES

[1] M. Ahmad, A. Hameed, A. A. Ikram and I. Wahid, "State-of-the-Art Clustering Schemes in Mobile Ad Hoc Networks: Objectives, Challenges, and Future Directions," *in IEEE Access*, vol. 7, pp. 17067-17081, 2019.

[2] C. Cooper, ‘‘Apples cook: 172 million post-PC devices in the last year,’’ CNET, New York, NY, USA, Tech. Rep., Mar, 2012.

[3] Rendong Bai and M. Singhal, "DOA: DSR over AODV Routing for Mobile Ad Hoc Networks," *in IEEE Transactions on Mobile Computing*, vol. 5, no. 10, pp. 1403-1416, Oct, 2006.

[4] J. J. Ferronato and M. A. S. Trentin, "Analysis of Routing Protocols OLSR, AODV and ZRP in Real Urban Vehicular Scenario with Density Variation," *in IEEE Latin America Transactions*, vol. 15, no. 9, pp. 1727-1734, 2017.

[5] S. Sarkar and R. Datta, "Mobility-aware route selection technique for mobile ad hoc networks," in *IET Wireless Sensor Systems*, vol. 7, no. 3, pp. 55-64, 6 2017.

[6] Eriksson J, Faloutsos M, Krishnamurthy S. Routing scalability in MANETs. University of California, Riverside. 2005.

[7] R. Neogy, C. Chowdhury and S. Neogy, "A reliable service discovery protocol using mobile agents in MANET," 2012 Proceedings Annual Reliability and Maintainability Symposium, Reno, NV, pp. 1-7, 2012.

[8] S. Marwaha, Chen Khong Tham and D. Srinivasan, "Mobile agents based routing protocol for mobile ad hoc networks," *Global Telecommunications Conference*, 2002. GLOBECOM '02. IEEE, Taipei, Taiwan, pp. 163-167 vol.1, 2002.

[9] M. B. Channappagoudar and P. Venkataram, "Mobile agent based node monitoring protocol for MANETs," *2013 National Conference on Communications (NCC)*, New Delhi, India, pp. 1-5, 2013.

[10] K. Tei, N. Yoshioka, Y. Fukazawa and S. Honiden, "Geographically bound mobile agent in MANET," *The Second Annual International Conference on Mobile and Ubiquitous Systems*: Networking and Services, San Diego, CA, USA, pp. 516-518, 2005.

[11] Talwar, B., Venkataram, P. & Patnaik, L.M. Wireless Pers Commun 41: 301. https://doi.org/10.1007/s11277-006-9144-4, 2007.

[12] L. Liang and P. Graham, "Assessment of a Mobile Agent Based Routing Protocol for Mobile Ad-hoc Networks," *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)*, Niagara Falls, Ont., pp. 1-5, 2007.

[13] Lauf AP, Peters RA, Robinson WH. “A distributed intrusion detection system for resource-constrained devices in ad-hoc networks”. Ad Hoc Networks. Vol, 8, no. 3, pp. 253-66, May 2010.

[14] W. G. Theresa and S. Sakthivel, "Fuzzy based intrusion detection for cluster based battlefield MANET," *2017 IEEE International Conference on Smart Technologies and Management for Computing*, Communication, *Controls, Energy and Materials (ICSTM)*, Chennai, pp. 22-27, 2017.

[15] L. Li and R. Liu, "Securing Cluster-Based Ad Hoc Networks with Distributed Authorities," in *IEEE Transactions on Wireless Communications*, vol. 9, no. 10, pp. 3072-3081, October 2010.

[16] T. Tsuda, Y. Komai, T. Hara and S. Nishio, "Top-k Query Processing and Malicious Node Identification Based on Node Grouping in MANETs," *in IEEE Access*, vol. 4, pp. 993-1007, 2016.

[17] Wang, Na, and Jian Li. "Shortest Path Routing With Risk Control for Compromised Wireless Sensor Networks." *IEEE Access*, vol. 7, pp. 19303-19311, 2019.

[18] Shehada, Dina, Chan Yeob Yeun, M. Jamal Zemerly, Mahmoud Al-Qutayri, Yousof Al-Hammadi, and Jiankun Hu. "A new adaptive trust and reputation model for mobile agent systems." *Journal of Network and Computer Applications*, vol 124, pp. 33-43, 2018.

[19] Harrabi, Samira, Ines Ben Jaafar, and Khaled Ghedira. "Message dissemination in vehicular networks on the basis of agent technology." *Wireless Personal Communications*, vol 96, no. 4, pp 6129-6146, 2017

[20] Rohankar, Rupali. "Agent based predictive data collection in opportunistic wireless sensor network." *Procedia Computer Science*, vol 57, pp. 33-40, 2015.

[21] Abosamra, Ahmed, Mohamed Hashem, and Gamal Darwish. "Securing DSR with mobile agents in wireless ad hoc networks." *Egyptian Informatics Journal*, vol. 12, no. 1, pp. 29-36, 2011.

[22] Halim, Islam Tharwat A., Hossam MA Fahmy, Ayman M. Bahaa El-Din, and Mohamed H. El-Shafey. "Agent-Based Trusted On-Demand Routing Protocol for Mobile Ad Hoc Networks." *In 2010 Fourth International Conference on Network and System Security*, pp. 255-262. IEEE, 2010.
[23] García-Magariño, Iván, Raquel Lacuesta, and Jaime Lloret. "*Agent-based simulation of smart beds with Internet-of-Things for exploring big data analytics*." IEEE Access, vol. 6: 366-379, 2018.
[24] Fortino, Giancarlo, Wilma Russo, Claudio Savaglio, Weiming Shen, and Mengchu Zhou. "Agent-oriented cooperative smart objects: From IoT system design to implementation." *IEEE Transactions on Systems, Man, and Cybernetics*: *Systems*, vol. 99, pp. 1-18, 2017.
[25] Gargees, Rasha S., and Grant J. Scott. "Dynamically Scalable Distributed Virtual Framework Based on Agents and Pub/Sub Pattern for IoT Media Data." *IEEE Internet of Things Journal6*, no. 1, pp. 599-613, 2019.
[26] Quan, Yue, Wen Chen, Zhihai Wu, and Li Peng. "Distributed fault detection for second-order delayed multi-agent systems with adversaries." *IEEE Access*, vol. 5, pp. 16478-16483, 2017.
[27] Wang, Dong, and Wei Wang. "Distributed fault detection and isolation for discrete time multi-agent systems." In *Computational Intelligence, Networked Systems and Their Applications*, pp. 496-505. Springer, Berlin, Heidelberg, 2014.
[28] Fortino, Giancarlo, Raffaele Gravina, Wilma Russo, and Claudio Savaglio. "Modeling and simulating Internet-of-Things systems: A hybrid agent-oriented approach." *Computing in Science & Engineering*, vol. 19, no. 5, pp. 68-76, 2017.
[29] Santos, João, Joel JPC Rodrigues, João Casal, Kashif Saleem, and Victor Denisov. "Intelligent personal assistants based on internet of things approaches." *IEEE Systems Journal*, vol. 12, no. 2, pp. 1793-1802, 2018.
[30] Hsieh, Han-Chuan, Kai-Di Chang, Ling-Feng Wang, Jiann-Liang Chen, and Han-Chieh Chao. "ScriptIoT: A script framework for and internet-of-things applications." *IEEE Internet of Things Journal*, vol. 3, no. 4, pp. 628-636, 2015.
[31] S. Lu, L. Li, K. Lam and L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack," *2009 International Conference on Computational Intelligence and Security*, Beijing, pp. 421-425, 2009.
[32] P. Papadimitratos and Z. J. Haas, "Secure link state routing for mobile ad hoc networks," *2003 Symposium on Applications and the Internet Workshops, 2003. Proceedings*, Orlando, FL, USA, pp. 379-383, 2003.

BIOGRAPHIES OF AUTHORS

Chethan B.K is working as assistant professor department of information science and engineering in Sri Siddhartha Institute of Technology, Tumkur, India. He has around 12 years of teaching experice. His research domains are computer network, network security and software engineering. Currently, He is pursuing his phd from VTU, Belagavi, India

Dr. M. Siddappa is working as a dean academics, professor and head department of computer science and engineering in Sri Siddhartha Institute of Technology, Tumkur, India. He has total number of experience is 30 years. His research domains are computer network, Artificial Intelligence, Soft Computing and agent based systems.

Dr. H S Jayanna is working as a professor and head department of information science and engineering in Siddaganga Institute of Technology, Tumkur, India. He has total number of experience is 25 years. His research domains are computer networks, Pattern recognition, Image processing, Continuous speech recognition and Speaker Identification/Verification using speech.