Friendly Group Architecture for Securely Promoting Selfish Node Cooperation in Wireless Ad-hoc Network

Rajani K C[1], Dr Aishwarya P[2], Manjunath S[3]
Assistant Professor, Department of Artificial Intelligence and Machine Learning, Cambridge Institute of Technology, Bangalore[1]
Prof and HOD, Department of CSE, Atria Institute of Technology, Bangalore[2]
Associate Professor, Department of CSE, Cambridge Institute of Technology, Bangalore[3], India

***Abstract*—Wireless Ad-hoc Network is characterized by a decentralized communication scheme with self-configuring nodes which has witnessed a wide range of practical wireless applications. However, this characteristic also results in various security threats in vulnerable wireless environment irrespective of presence of various routing protocols. Review of existing literatureshows that there is very less emphasis towards securing Dynamic Source Routing (DSR) while majority of solutions uses encryption- based operation. Therefore, this manuscript introduces a novel non-encryption-based scheme called as Friendly Group Architecture which intends to identify the presence of selfish node followed by presenting a method to promote the secure cooperation of it. The complete modelling is analytically designed using probability-based computation and dynamic thresholding. The simulation outcome carried out in MATLAB exhibits that it outperforms existing system with respect to energy, overhead, andsecurity.**

Keyword*—Wireless Adhoc network; selfish node; DSR; reactive;security

I. INTRODUCTION

A wireless adhoc network is basically a decentralized form of network system where the devices are connected via wireless medium without any dependencies of infrastructure [1]. The decision of routing is undertaken by all the individual wireless nodes carried out dynamically using a routing protocol [2][3]. They can be stated as a self-configuring network with dynamic capabilities. There is no restriction of mobility for such device as the links changes frequency with other connected devices. While doing so, the elementary challenge is to prepare each wireless node to manage information that is demanded for a proper connection [4][5]. This give rises to more challenges as there is a need to forward the data packet to almost all the nodes which comes in the vicinity of its transmission zone. Apart from this, another challenge will be to maintain a required proportion of overhead under control for better routing performance [6]. Although, each nodes is aware of its own data transmission performance but they have no much idea about the demands of others. Apart from this, the dependencies of limited channel capacity are another impediment towards data transmission. Wireless adhoc network is always under a constant threat of attackers owing to its spontaneously changing topology. All the security threats that are present in conventional network are also applicable in wireless ad-hoc network with respect to authentication, confidentiality, integrity, privacy, etc. [7]-[9]. Owing to such security threats, there are an increasing occurrences of intrusion events e.g., inferior monitoring of routing, denial of service attack, injection of counterfeited message, eavesdropping, etc. Essentially, there are two types of routing scheme widely deployed i.e., proactive and reactive protocols. It is found that proactive protocols are (e.g., optimized link state routing, destination sequence distance vector) are more prone to get compromised compared to reactive schemes (e.g., adhoc on-demand distance vector, dynamic source routing). A closer look into existing approaches also showcase that majority of the security scheme is carried out over reactive protocols and currently more research is also dedicated towards securing proactive protocols. However, there are less studies being carried out securing a variant of reactive protocol i.e. Dynamic Source Routing (DSR) to construct on-demand routes while forwarding request of node using source routing. The significant advantage of DSR is its independence from forwarding table update beacon periodically. The overhead is significantly controlled using cache information of route in DSR. However, majority of the security threat in DSR arises from its incapability to repair broken links while lack of updated cache information accelerates to this problem further more. DSR protocol is more prone to flooding attack and it could result in higher delay during connection set up compared to other proactive protocols. Apart from this, DSR protocols is actually meant for static environment and environment with low mobility to some extent [10][11]. They are not suitable for handling communication with higher degree of mobility.

1) Motivation behind the study: With the number of application rising towards the usage of ubiquitous computing, it is necessary that such forms of application should be smart enough to identify threat. However, adoption of sophisticated mechanism may significantly assist in threat detection but at the cost of computational and network resources. Adoption of DSR protocol offers beneficial networking perspective but their mechanism of inherent source routing makes the nodes more vulnerable towards it identity. This is the prime motivational factor to carry out the study towards improving DSR protocol in order to incorporate a capability to perform

secure routing operation in presence of routing misbehavior event in wireless adhoc network.

2) Study contribution: Apart from this, it is also seen that irrespective of various studies towards securing wireless adhoc network, there is no benchmarked model which can ascertain this fact. Therefore, the proposed system presents a novel scheme called as Friendly Group Architecture, which uses a simplified analytical model using probability theory exploits the selfish node to promote selfish node cooperation. The study contributes towards a novel modelling of securing DSR protocol by identifying selfish node as well as promotes cooperation of selfish nodes in presence of unknown malicious environment. The core idea of this framework is to balance the security, resource, and overhead demands to enhance DSR protocol in wireless adhoc network. Therefore, the study contribution is as follows:

- The proposed model is developed on the basis of an adversarial model whose information is not predefined with the other normal nodes in network.
- The model presents friendly group architecture which uses both normal and selfish node to participate in data forwarding process.
- The proposed technique introduces a unique incentive allocation scheme which is allocated to all the nodes on the basis of their undertaken action.
- The incentive policy is meant for promoting selfish node to achieve gain if they choose to forward data as a normal node.
- The proposed model is capable of resisting majority of the routing misbehavior in wireless adhoc network with better data transmission performance being noted.

The organization of this paper is as follows: Section II discusses about the existing literatures where different techniques are discussed for detection schemes used in power transmission lines followed by discussion of research problems in Section IIIand proposed solution in IV. Section V discusses about algorithm implementation followed by discussion of result analysis in Section VI and discussion in Section VII. Finally, theconclusive remarks are provided in Section VIII.

II. Related Work

This section briefs of existing approaches towards security in wireless adhoc network especially emphasizing on the work carried out using routing protocols. The work of Almazok et al. [12] have presented an optimized version of DSR protocol using bio-inspired approach as well as time scheduling with main focus on routing performance. Study towards similar direction of improving routing performance is also carried out by Berri et al. [13] where a statistical modelling has been carried out using state of links. Study towards anomaly detection is carried out by Chugh et al. [14] wgere a zone-driven data forwarding scheme has been introduces. Existing study has also discussed about the resistivity techniques against selfish node using reputation based DSR protocol considering the mobility aspect of it as witness in work of Delgado et al. [15]. Hadi et al. [16] have further presented a work which can enhance the detection performance of selfish node under mobility environment using on-demand routing scheme. Study of Liang et al. [17] have presented a DSR scheme by filtering the optimal path for routing to offer more reliable data delivery performance. The work of Mohan Priya et al. [18] have presented a secured DSR scheme in order to resist a specific form of attack i.e. black hole attack. Study towards selfish nature of vehicular network system is investigated by Shan et al. [19] considering static and dynamic nature of the node over multiple environments of communication. The work carried out by Shan et al. [20] has presented a discussion about influence of energy dissipation towards selfish behaviors in mobility environment. Exclusive study towards securing mobility environment is carried out by Srivastava et al. [21] where digital signature is used for authenticating the participating nodes. Azam et al. [22] have studied about various authentication scheme over vehicular adhoc network while work of Faisal et al. [23] have presented a detection of identity attack in wireless adhoc network considering received signal strength. Farahani [24] have used k-nearest method for computing reputation in order to resist black hole attack over mobility environment. Im and Lee [25] have presented a secure covert communication system over two hop adhoc network. Mahmood et al. [26] have studied the issues associated with existing security scheme over vehicular adhoc network and concludes that there are still many issues which require attention in conventional scheme. Naresh et al. [27] have used group key agreement for securing cluster-based communication in adhoc network. Usage of blockchain is reported in work of Ran et al. [28] where on-demand data transmission scheme is used considering QoS constraint. Siddiqui et al. [29] have presented a security approach for resisting wormhole and blackhole attack considering adhoc network integrated with an Internet-of- Security. Wu et al. [30] have presented a secure authentication scheme using key exchange protocol over vehicular adhoc network. Hence, it can be noticed that there are some dedicated investigations towards securing wireless adhoc network. The next section briefs about the issues associated with existing system of secure routing scheme in wireless adhoc network.

1) Limitation and research gap: The prime limiting factors of existing security techniques are mainly associated with the core emphasis on adopting sophisticated technique to identify abnormality in routing. The techniques are either based on data forwarding or it's based on high-end resource dependent securitytechnique. Another significant limiting factor is that the solution of problem space is more concerned about singular form of attack. Such methodologies make the system non-applicable in different attack scenario. Hence, there is potential research gap between rising of dynamic adversaries and existing problem solution, which is highly symptomatic to specific event. Hence, they cannot be deployed over the scenario which calls for presence of multi-attacker or attackers launching dynamic strategies of attack in wireless adhoc network. Apart from this,there is a still a gap between security solution resiliency and itsdependencies towards resources.

III. RESEARCH PROBLEM

The unaddressed problems explored after reviewing the existing system are as follows:

- There are very few potential implementations towards securing DSR protocol over uncertain condition of intrusionin wireless adhoc network.
- Majority of the existing security approaches are based on authentication on priorly known information of the attackerand they are highly specific for attackers.
- The fact that attacker could exhibit dynamic behavior is out of scope of any existing implementation work in wireless adhoc network.
- Existing security approaches doesn't offer much balance between data transmission performance and securityperformance at a same time.

Therefore, the problem statement arrived from the above points is "Developing a novel secure data transmission scheme considering the dynamicity of attacker behaviors and harnessing malicious node to secure communication in wireless adhoc network is challenging task".

IV. RESEARCH METHODOLOGY

The core target of the proposed system is to introduce friendly group architecture in order to secure DSR protocol in wireless adhoc network. The secondary objective of this architecture is also to ensure better resource management alongwith overhead reduction. The term 'friendly' is stated as this architecture offers identification of selfish node and uses them in order to perform data dissemination in uncertain communication environment in presence of uncertain intruder'sstrategy. Fig. 1 highlights the proposed architecture.

A closer look in Fig.1 shows that proposed DSR implementation scheme is classified into two functionalities i.e., identification of selfish node followed by secure participation of selfish node. In initial operation, all the response-based beacons are analyzed in order to compute probability of cooperation as well as intrusion. These two parameters are further used for computing two empirical forms of trust i.e., degree of conformity which is about data forwarding operation and degree of non- conformity which is about rejecting all possibilities of forwarding data (followed by dropping packet). Further conditions are designed to finalize the trust value from its third type i.e., degree of vagueness in trust, which is about incapability of a node to decide if the other node is regular or selfish node. Finally using dynamic thresholding, selfish node is positively identified. The next round of operation is to further assess the probability of attacker identity for the selfish node followed by another dynamic thresholding in order to allocate incentives. All selfish nodes that comply with proposed secured DSR protocol will be allocated a measurable incentive in order to promote selfish node cooperation. The proposed system ensures that under no circumstances, the selfish nodes once identified as positive attacker will be able to initiate attack next time. The next section discusses algorithms.

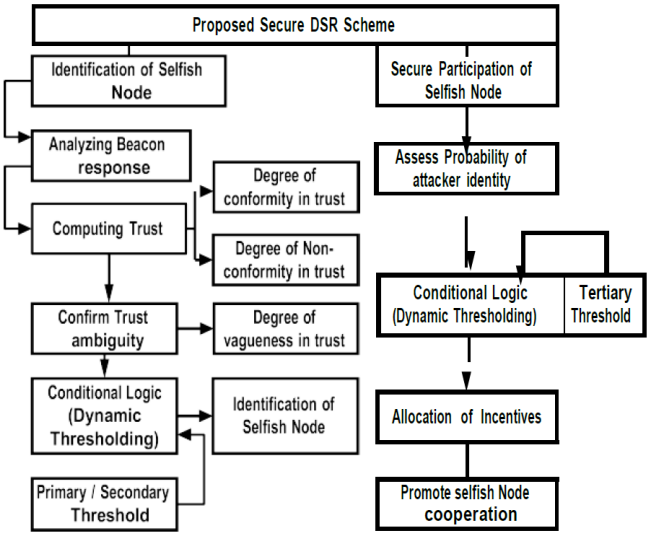

Fig. 1. Proposed friendly group architecture.

V. ALGORITHM IMPLEMENTATION

This section discusses about the algorithm design and its implication towards developing friendly group architecture with an implicit focus on identification of a selfish node and ensuring participation of a selfish node securely. The novelty of the algorithm implementation is that it exploits the selfish node to participate in data forwarding process even after positively identifying it as a selfish node. This is completely different from any existing system which either isolates the selfish node or takes countermeasure of its non-participation. However, the core idea of this algorithm is to incorporate security in DSR protocolusing retaliation-based concept within the node properties. The discussion of the algorithms is as follows:

A. Algorithm for Identification of Selfish Node

This algorithm is responsible for performing positive identification of a selfish node assuming that it doesn't have anypreviously fed information about its presence. The steps of the algorithm are as follows:

Algorithm for Identification of Selfish Node

Input: n (number of nodes)

Output: n_S (identified selfish node)

Start

1. **For** i=1:n
2. $n_{ad} \rightarrow n_t$(RREP)
3. n_t computes d_C and d_{nC}
4. **If** $d_{nC} > d_C$ & $d_{nC} > T1$
5. n_S=declare n_{ad} as selfish node
6. **If** (p_C=pa)
7. compute d_V
8. **If** $d_V > T2$
9. n_S=declare n_{ad} as selfish node
10. *End*
11. **End**

The algorithm takes an input of n (number of nodes) which after processing yields an outcome of ns (identified selfish node). Considering all the nodes n in simulation area (Line-1), the adjacent node nad forwards the route response beacon RREP to the transmitting node nt after the former receives the route request message from latter (Line-2). Upon receiving this beacon, the transmitting node nt computes degree of conformity in trust dc as well as degree of non-conformity of trust dnc (Line- 3). For a regular form of node, the frequencies of dnc value should reduce or stop which is not the case of malicious form of node. This is because the malicious node could have opted for initially forwarding the regular response in order to increase its individual trust value. In such case, it could become quite impossible for the transmitting node to decide if the adjacent node is regular node or malicious node. Hence, the computation of dc and dnc assist in this regard in the form of mathematical expression as follows:

$$dc = pc / pc + pa$$

$$dnc = pa / pc + pa \quad (1)$$

In the above expression (1), μ_1 and μ_2 represents probability of cooperation (forwarding data) or probability of intrusion respectively. For any discrete value of p_c and p_a, it's easier to find the case of vulnerability where in such case dnc>>dc. However, if the attacker chooses to increase its trust value by cooperating than in such case, pc= pa which will result in dc=dnc (Line-6). This similar value of degrees will lead to failure of decision of nodes about the regularity and malicious nature. The proposed system considers a primary threshold T_1 which is assigned by user to becompared with d_{nc} (Line-4) to determine its malicious nature (Line-5). However, in case of Line-6, the proposed algorithm further computes degree of vaguess mathematically as follows:

$$d_v = (\lambda . P_1)/(P_2.P3) \quad (2)$$

In the above expression, the variables λ, P1, P2, and P3 represents network coefficient, (pc*pa), $(pc+pa)^2$, and (pc+pa+1) respectively. This mathematical expression is used only in the condition stated in Line-6. After the dv value is obtained, its is further compared with secondary threshold T2 to ensure that dv should be always within T2 limit (Line-8) otherwise, the monitored adjacent node is termed as malicious node (Line-9). It should be noted that proposed algorithm represents selfish node as malicious node. For regular environment, the value of dv should be reduced and its value is fixed by user based on the application it deploys. Hence, using a simplified probability concept, proposed system can easily identify selfish node ns.

B. Algorithm for Secure Participation of Selfish Node

This algorithm is a continuation of the previous algorithm which detects the selfish node. The prime basis of this algorithm are two folds viz. i) a selfish node will not introduce any form of attack in the preliminary level and will choose to cooperate. As selfish node will not be aware of security protocol running, this is the best way to get them latently introduced within the network, gain trust, and introduce attack, ii) selfish node also participate in data forwarding process; however, they do it with malicious intention. Hence, the above two properties can be harnessed to exploit the data forwarding capability of selfish node as a complimentary to regular node for seamless secure data transmission. However, this operation is strictly monitored on the basis of threat computation for such selfish node and until and unless they are within a permissible limit, the selfish nodes are allowed to propagate data. The success factor of this algorithm completely depends upon how positively the first algorithm works. Apart from this, a second level of controlling is offer, by allocating incentives to the nodes based on their adopted steps of action, the proposed algorithm offers secure participation of selfish nodes. The operational steps of the proposed algorithm are as follows:

Algorithm for Secure Participation of Selfish Node

Input: n_S (selfish nodes)

Output: S_p (secure participation)

Start

1. **For** i=1: ns
2. compute $p$aid of n_S
3. **If** $p$aid>T3
4. Allocate $I_1 \rightarrow n_S$
5. *Else*
6. S_p=Allocate $I_2 \rightarrow n_S$
7. *End*
8. update S_p, d_v, d_c, and d_{nc}
9. *End*

This above stated algorithm takes the input of ns (selfish nodes) from prior algorithm which after processing ensures an outcome of Sp (secure participation). This algorithm considers all the ns (selfish nodes) (Line-1) followed by conditional assessment to check if the probability of attacker paid is greater than tertiary threshold T3 (Line-3). It should be noted that proposed system performs computation of paid using same expression as that of pa as seen in prior algorithm. If the paid value is found to be more than T3 than it will represent positive presence of many numbers of selfish node. Knowing that fact that a selfish node will need to comply with the proposed secure DSR protocol and hence, its actions will be controlled by allocating an incentive I1, which are computed based on their trust value. The incentive I1 will state allocating of increasing number of profits for selfish node as long as they assist in forwarding data. However, there is also a possibility that the selfish node violates proposed secure DSR protocol and executes its own malicious code. In such case, the malicious node's action is public-ally flagged as a malicious node to all other regular node and in such case; it fails in further data forwarding process to other non-victim regular node. Hence, the selfish node has no other option but to assists in data forwarding or else they will need to isolate themselves from the current network itself (Line- 4). On the other hand, if paid value is found to be lower than tertiary threshold than they are allocated an incentive of I2. It should be noted that I2>I1, which is strategically designed to ensure participation of selfish node (Line-6). All the other variables are further updated and this updated information is shared among all the neighboring nodes (Line-8).

It is to be noted that prime contribution of the proposed secured DSR protocol is basically in the formulation of the incentives which directly control the actions of all nodes on the basis of their actions viz. i) data forwarding, ii) data dropping, iii) raising a notification about intrusion, and iv) introducing intrusion. It could be seen that first two actions could be exhibited by both regular node and selfish node whereas the discrete action of third and fourth could be only exhibited by regular node and selfish node respectively. Hence, on the basis of dv value computation, observing its trend, and comparing with the threshold value. In this process, there is also a likelihood that a regular node could generate false alarm and hence the proposed system introduces an inclusion of penalty factor which is computed for every decision of alarm generated by the regular node. Although, there is a possibility of few instances of false alarm by regular node, but more the regular node updates its variable (Line-8), the occurrences of such false alarm reduces down and network becomes more accurate to capture the event of intrusion. Apart from this, a non-inclusion of conventional cryptography approach is one big advantage of proposed system which not only makes the proposed DSR protocol to offer security but also leverages the data transmission performance in wireless adhoc network.

VI. Result Analysis

This section discusses about the implementation of the proposed system discussed in prior section using MATLAB. The simulation environment consists of randomly distributing 500 nodes in 1000x1000 m2 area with 3000 simulation rounds. The assessment of performance is done using 4 evaluation parameters i.e., overhead, battery usage, identification of selfish node, and consistency in selfish node cooperation. The outcome of proposed system is compared with current work of Delgado et al. [15] termed as DRSR and conventional DSR protocol.

Fig. 2 highlights the traffic overhead reduction which is computed as proportion of control message that lacks application contents. Owing to possession of stale route information, DSR protocols exhibits higher traffic overhead in case of unnecessary cooperation by selfish node, which is avoided to a large scale in DRSR scheme which uses allocation of reputation value for establishing communication. However, DRSR considers static nodes which further doesn't scale up when the iteration is incremented. Proposed system, on the other hand, ensures all its routing decision on the basis of computed probabilities of trust. This ensures higher generation of reliable links causing higher reduction of traffic overhead.

Fig. 3 highlights the battery saving where proposed system excels better energy saving compared to proposed system. Both existing system of DSR and DRSR make use of highly iterative mechanism to find the routes with more emphasis over the destination node proximity and not much into ascertaining the reliability of neighboring node. This is the reason that both the existing schemes doesn't have much significantly different outcomes of battery saving. On the other hand, proposed system has highly structured computation of links, where thresholding, updating operation, and computation of threat probability are spontaneous causing efficient and secure route. This leads to significant energy saving.

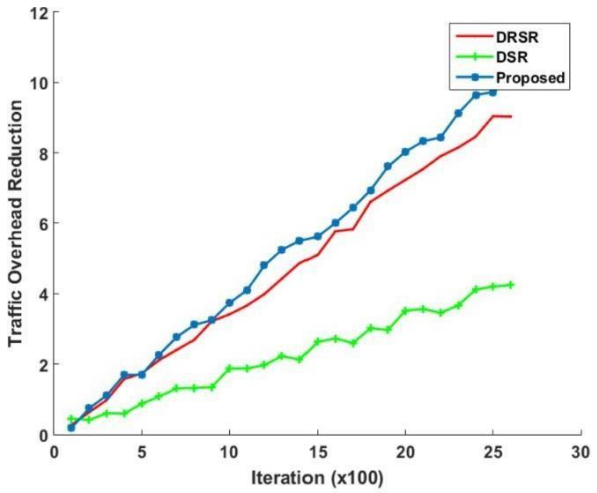

Fig. 2. Analysis of traffic overhead reduction.

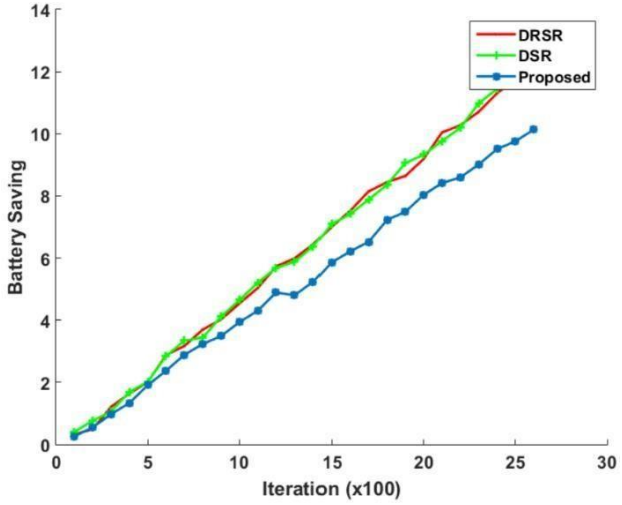

Fig. 3. Analysis of battery saving.

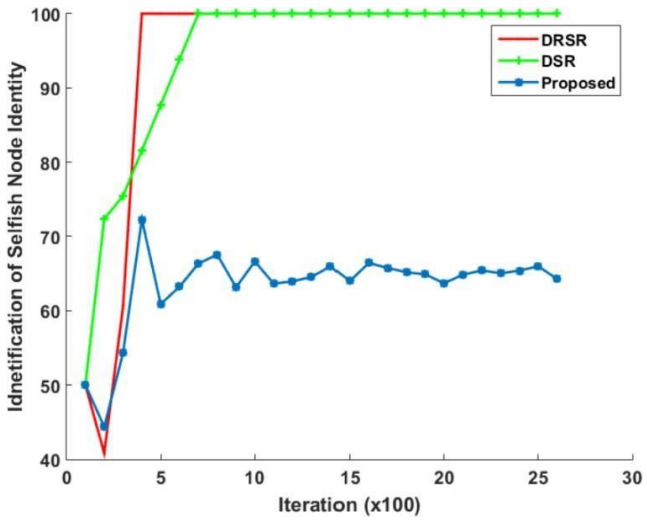

Fig. 4. Analysis of identification of selfish node identity.

Fig. 4 highlights the positive identification of selfish node. It should be noted that proposed system uses three different forms of thresholds in order to confirm the identity of selfish node and therefore, although the trendline of proposed system is lower than existing system, but still the outcome is reliable to consider in presence of uncertain and dynamic environment. This is because, existing DSR and DRSR system showcase higher identification rate as its attackers are well defined in its environment and hence this outcome is not applicable for uncertain intrusion environment.

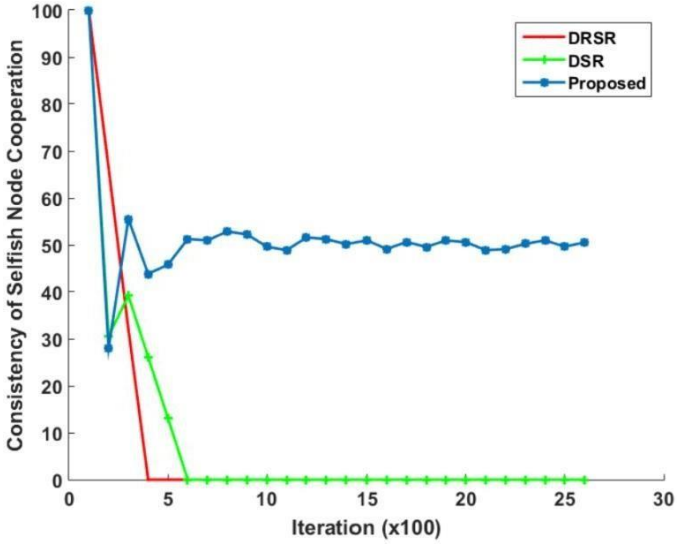

Fig. 5. Analysis of consistency of selfish node cooperation.

Fig. 5 highlights the consistency of the selfish node cooperation. In this case, it is proved that existing system doesn't support selfish node cooperation, where amending the conventional DSR in proposed system logic entails that selfish node has no other choice but to participate in data forwarding process in proposed friendly group architecture. A closer look into the graphical trend shows that proposed system has superior consistency with an increase of iteration. This is because of the fact that proposed algorithm performs spontaneous updates which not only reduces the effort to compute degree of vagueness in trust but it also increases degree of conformity of trust resulting. Allocation of dual form of incentives either forces the selfish nodes to participate till it drains its energy or it isolates the selfish node if the probability of attacker identity is found to be highly significant. Although, this may cause selfish node slightly bypassing the security in preliminary level (0-less than 5 round), however, it soon obtains its consistency and hence proposed system offers more reliable outcomes with respect to selfish node cooperation.

VII. Discussion

From the previous section, it is quite evident that proposed scheme offers better performance in contrast to existing routing schemes. There are multiple points to be highlighted for this perspective of outcomes which are as follows:

- Overhead control is one of the potential contributions of proposed scheme. A closer look into the friendly architecture in joint collaboration with incentive policy states that proposed system carry out its operation on the basis of three different forms of trust scores. This computation is carried for each group in friendly architecture using probability-based conditional logic. Hence, there is much less effort implied by proposed scheme towards trust computation whereas existing DRSR scheme is required to iteratively compute trust score. This fact doesn't suit well in presence of dynamic environment leading to higher traffic overhead in DRSR. At the same time, the higher score of traffic overhead in DSR is accounted for its increasing memory allocation to retain source information.
- From the resource consumption viewpoint, the only operation proposed scheme does are dual fold viz. i) trust computation by neighborhood monitoring and ii) allocation of incentives using conditional logic. The complete operation requires lesser memory, is faster, and is always updated causing better resource retention performance of proposed system with increasing iteration. This is not the case with DSR or DRSR or any other existing scheme briefed in Section II.
- From the security perspective, the proposed scheme emphasized on identification of selfish node on the basis of presented trust computation. The granularity in the trust computation is further ensured by progressive assessment of conditional logic based on dynamic thresholding. This causes uniform performance of selfish node identification over increasing iteration. However, existing scheme e.g. [12]-[25] considers highly sophisticated computation while scheme [26]-[30] offers highly iterative scheme that captures attacker only if attack definition is well defined. Hence, the inconsistency arises in selfish node identification with increasing iteration witnessed with dynamic topology.
- One of the major contributions of the proposed scheme is its prevention technique where the positively identified selfish node is forced to cooperate in network. It is also quite fair enough to ascertain that at certain point of time, such selfish node could violate too. However, there are very less chances for this as if the selfish node chooses to violate, its information have already been updated in hop table of all its neighboring nodes. In such case, selfish node will fail to initiate a new attack in different group. Apart from this, the neighborhood monitoring is a continuous process which is also responsible of capturing any form of anomaly in behaviour of selfish node causing routing misbehaviour.

VIII. Conclusion

The presence of intruder in wireless adhoc network is quite challenging to be explored even by the most potential intrusion detection system. Existing studies carried out considers the predefined information about the attacker doesn't find its applicability over dynamic form of network.

Apart from this, there was so significant security work being carried out considering DSR protocol. These challenges are addressed in current study with following contributions: i) a novel analytical framework of Friendly Group Architecture which promotes the regular node to perform seamless data transmission as well as promotes selfish node for secure cooperation, ii) every actions of selfish nodes are preemptively computed in order to find out its next step of actions and accordingly allocation of incentives are carried out, iii) the proposed model is completely independent of any apriori information of an attacker and hence it can be widely applicable for resisting majority of attacks, iv) the proposed model offers a well-balance between traffic overhead, energy consumption, and security.

REFERENCES

[1] A.H. Wheeb, M.T. Naser, "Simulation based comparison of routing protocols in wireless multihop ad hoc networks", International Journal of Electrical and Computer Engineering, Vol. 11, No. 4,pp. 3186~3192, 2021.

[2] Alamsyah, I K.E. Purnama, E. Setijadi, M. H. Purnomo, "MPR selection to the OLSR quality of service in MANET using minmax algorithm", International Journal of Electrical and Computer Engineering, Vol. 9, No. 1, pp. 417~425, 2019.

[3] Y. Khamayseh, M. B. Yassein, M. Abu-Jazoh, "Intelligent black hole detection in mobile AdHoc networks", International Journal of Electrical and Computer Engineering, Vol. 9, No. 3, pp. 1968~1977, 2019.

[4] J.Mahmood, Z. Duan,Y.Yang, Q. Wang,J. Nebhen, and M.N.M. Bhutta, "Security in Vehicular Ad Hoc Networks: Challenges and Countermeasures", Hindawi Security and Communication Networks, 2021.

[5] Mohammad Al mojamed, "Integrating Mobile Ad Hoc Networks with the Internet Based on OLSR", Hindawi-Wireless Communications and Mobile Computing, 2020.

[6] S.Prabhavat,W.Narongkhachavana,T.Thongthavorn,and C. Phankaew, "Low Overhead Localized Routing in Mobile AdHoc Networks", Hindawi-Wireless Communications and Mobile Computing, 2019.

[7] H. Amraoui, A. Habbani, A. Hajami, and E. Bilal, "Security-Based Mechanism for Proactive Routing Schema Using Game Theory Model", Hindawi Publishing Corporation Mobile Information Systems, 2016.

[8] Y. Mao, C. Zhou, J. Qi, and X. Zhu, "A fair credit-based incentive mechanism for routing in DTN-based sensor network with nodes' selfishness", EURASIP Journal on Wireless COmmunications and Networking, 2020.

[9] Y. Lv,"Security Issues in Multi-hop Device-to-device Communication Networks - Secure Routing Protocols Solution", Journal of Physics: Conference Series, vol.1828, 2021.

[10] H. Yang, "A Study on Improving Secure Routing Performance Using TrustModel in MANET", Hindawi-Mobile Information Systems, 2020.

[11] M. I. Idris, A. Hadi Abd Rahman, P-C Lin, and P. C. K. Hung, "Life Expectancy Analysis of DSR and DSDV Protocol in MANET with Dos Attack", International Journal of Computer Science and Network Security, VOL.20 No.3, March 2020.

[12] S. A. Almazok and B. Bilgehan, "A novel dynamic source routing (DSR) protocol based on minimum execution time scheduling and moth flame optimization (MET-MFO)", EURASIP Journal on Wireless Communications and Networking, 2020.

[13] S. Berri, S. Lasaulce, and M. S. Radjef, "Efficient packet transmission in wireless ad hoc networks with partially informed nodes", EURASIP Journal on Wireless Communications and Networking, vol.148, 2019.

[14] N. Chugh, G. S. Tomar, R. S. Bhadoria, and N. Saxena, "A Novel Anomaly Behavior Detection Scheme for Mobile AdHoc Networks", MDPI-Journalon Electronics, vol.10, 2021.

[15] L. G. Delgado, E. P. Segarra, A. M. Mezher and J. Forné, "A novel dynamic reputation-based source routing protocol for mobile ad hoc networks", EURASIP Journal on Wireless Communications and Networking, vol.77, 2019.

[16] Ahmed. A. Hadi, Zulkarnain Md. Ali, Yazan Aljeroudi, "Improved Selfish Node Detection Algorithm for Mobile Ad Hoc Network", International Journal of Advanced Computer Science and Applications, Vol. 8, No. 4, 2017.

[17] Q. Liang, T. Lin, F. Wu, F. Zhang, W. Xiong, "A dynamic source routing protocol based on path reliability and link monitoring repair", PLOS ONEJournal, vol.16, Iss.5, 2020.

[18] M. Mohanapriya, N. Joshi, M. Soni, "Secure dynamic source routing protocol for defending black hole attacks in mobile Ad hoc networks",Indonesian Journal of Electrical Engineering and Computer Science, Vol. 21, No. 1, pp. 582~590, 2021.

[19] A. Shan, X. Fan, C. Wu and X. Zhang, "Quantitative Study on Impact of Static/Dynamic Selfishness on Network Performance in VANETs," in IEEE Access, vol. 9, pp. 13186-13197, 2021, doi: 10.1109/ACCESS.2021.3051976.

[20] A. Shan, X. Fan, C. Wu, X. Zhang, and S. Fan, "Quantitative Study on the Impact of Energy Consumption Based Dynamic Selfishness in MANETs", MDPI Journal on Sensors, vol.21, 2021.

[21] A. Srivastava, S. K. Gupta, M. Najim, N. Sahu, G. Aggarwal, and B. D. Mazumdar, "DSSAM: digitally signed secure acknowledgement method for mobile ad hoc network", EURASIP Journal on Wireless Communications and Networking, vol.12, 2021.

[22] F. Azam, S. K. Yadav, N. Priyadarshi, S. Padmanaban and R. C. Bansal, "A Comprehensive Review of Authentication Schemes in Vehicular Ad-Hoc Network," in IEEE Access, vol. 9, pp. 31309-31321, 2021, doi: 10.1109/ACCESS.2021.3060046.

[23] M. Faisal, S. Abbas, and H. Ur Rahman, "Identity attack detection system for 802.11-based ad hoc networks", EURASIP Journal on Wireless Communications and Networking, vol.128, 2018.

[24] G. Farahani, "Black Hole Attack Detection Using K-Nearest Neighbor Algorithm and Reputation Calculation in Mobile Ad Hoc Networks", Hindawi-Security and Communication Networks, 2021.

[25] H. -S. Im and S. -H. Lee, "Mobility-Assisted Covert Communication OverWireless Ad Hoc Networks," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 1768-1781, 2021, doi: 10.1109/TIFS.2020.3045132.

[26] J.Mahmood, Z.Duan, Y.Yang, Q.Wang, J.Nebhen, and M. N. M. Bhutta, "Security in Vehicular Ad Hoc Networks: Challenges and Countermeasures", Hindawi-Security and Communication Networks, 2021.

[27] V. S. Naresh, S. Reddi, and N.V.E.S. Murthy3, "A provably secure cluster-based hybrid hierarchical group key agreement for large wireless ad hoc networks", Springer Journal on Human-centric Computing and Information Science, vol.9, Iss.26, 2019.

[28] C. Ran, S. Yan, L. Huang, and L. Zhang, "An improved AODV routing security algorithm based on blockchain technology in ad hoc network", EURASIP Journal on Wireless Communication and Networking, 2021.

[29] M. N. Siddiqui, K. R. Malik and T. S. Malik, "Performance Analysis of Blackhole and Wormhole Attack in MANET Based IoT," 2021 International Conference on Digital Futures and Transformative Technologies (ICoDT2), 2021, pp. 1-8, doi: 10.1109/ICoDT252288.2021.9441515.

[30] T-Y Wu, Z. Lee, L. Yang, and C-M Chen, "A Provably Secure Authentication and Key Exchange Protocol in Vehicular Ad Hoc Networks", Hindawi-Security and Communication Networks, 2021.