Confide in Model with Delayed Verification for Message Handoff in VANETs

Sudhir Agrawal[1], Raj Kumar[2], Neeraj Kumar[3],Prateek Mishra[4],Shakun Garg[5]
[1]Buddha Institute of Technology, Gorakhpur sagarwal22@bit.ac.in
[2]Echelon Institute of Technology, Faridabad
rajkumar@eitfaridabad.co.in
[3]Raj Kumar Goel Institute of Technology, Ghaziabad
Nkp76fai@rkgit.edu.in
[4]Asia Pacific Institute of Information Technology SD India Panipat
prateekmishra@apiit.edu.in
[5]IIMT College of Engineering Greater Noida
shakun3956_gn@iimtindia.net

Abstract: With the advent of numerous types of attacks in wireless communication whether foreseen or unforeseen ones, it is a big challenge to build a trust in the VANETs for secure and reliable communication. The vast majority of the current trust models are personality based and utilize unreasonable intermittent trade between vehicles to fabricate a choice about trustiness of an interest vehicle. Noxious information can be limited in such models utilizing characters notoriety. When all is said and done, the nature of the information are not considered, regardless of a few models, which may repudiate messages in view of their temperament. Here we propose a different trust model for VANETs, where we provide recognition of attacks prior to the phase that begins the actual message interchange. The decision is made firm by considering the supposition of the last forwarder as well as the postponed confirmation of the traded message. We present another idea of sidekick vehicles, which is utilized to shift through and select the most confided in hubs among neighboring vehicles, to be utilized as transfers in the sending methodology. The arrangement of this system enable us to avert vehicles recognized as likely unscrupulous hubs from taking part in the system. We demonstrate that in the direst outcome imaginable, our trust result offers great outcomes.

Keywords: Trust Management, Intrusion Detection, Vehicular Ad-hoc Networks.

1 Introduction

VANETs are viewed as a critical segment of Intelligent Transportation Systems (ITS). It is VANET which enables multiple transport vehicles and street side units to communicate among themselves securely. In such systems it is the vehicles themselves that send a ready message to alert other vehicles in the network about the street activity or they may be utilized as a broadcaster of messages originating from the RSU or other vehicles in the network. To implement the similar objective we have seen an upsurge of research work in the past decade which focused on street wellbeing as well as voyager's increment in facility and security [1]. Be that as it may, the significance of VANET applications, what's more, Is the messages traded between vehicles can be immediately risked if at least trust is not given. Along these lines depending entirely on the supposition that, in such systems, all vehicles are reliable and helpful that may prompt undesirable circumstances particularly when a street security choice is made in light of a wrong data [2]. Subsequently, securing correspondences between hubs is basic for the arrangement of VANET applications. A few modal is proposed in this paper to resolve the distinctive parts of the dependability of the imparting hubs and the messages traded between them. One such modal handles known assaults utilizing On Board Unit (OBU) against DoS attack on the network [3]. In [4]the authors propose a security authorization convention, which depends on movement examination and assault discovery. A review exhibited in [5] proposes a validation strategy against best constrain attacks...etc. When all is said and done, trust relations depend on confirmation identified with the past co-operations of substances inside a convention. A VANETs trust model give an option to keep the exploitative hubs away from the network and include again in the mainstream hub when their trust build up to an acceptable level [6]. The primary classification criteria of the trust modals is based on genuineness of the participating vehicle while we have two other classification criteria [7][8][9]. The first classification is the one which is most elaborated and discussed in this paper. In this classification the models are related to the steering and security by forgoing the nature of messages. We consider the fact that a even genuine hub can also send malignant information. In the second-class

[10][11], models are propose to think about the traded information the information is sent by a fair hub. Be that as it may, the requirement for hubs to look at got messages against a database of legitimate activity may speak to an extra calculation overhead. At last, the third class contains cross breed models [12][13][14] where the proposed plans point at distinguishing and renouncing exploitative hubs and taking out malignant information from the system. Lately, these models acquire similar disadvantages caused by the past two classes. In this way, the confirmation procedure and framing an assessment about the genuineness of the message originators and the legitimacy of the message itself might be exceptionally requesting in wording of calculation time also the off message's overhead. In this paper, we propose an effective trust demonstrate which can identify and repudiate unscrupulous vehicles, and control malignant information construct just in light of the supposition of the last forwarder and utilizing a deferred check of the messages received. In this proposal, we present the worldview of sidekick vehicles, which permits our methodology to decide the briefest and most put stock in way to transfer the information parcels. By recognizing the most and best reliable transfer, a hub can abstain from choosing transfers with a high likelihood of unscrupulousness regardless of the possibility that they are on the most limited way to the goal. The rest of this paper is sorted out as takes after: In area II, we display a short audit of the fundamental existing confide in models. In segment III, we depict the points of interest of our demonstrate and depict the primary calculations utilized for building a supposition about the dependability of neighboring hubs what's more, Is the choice of the following bounce. In area IV, we depict our reenactment condition and talk about the outcomes got.And then At last, we give our closing comments in segment V.

2 Related Work

Related Work: One part of securing vehicular correspondence is through confide in models in VANETs, which goes for repudiating untrustworthy hubs from all interchanges and breaking down traded messages and erasing the pernicious ones. Trust models may be characterized into three classes: element situated, information arranged and crossover models [15].

2.1 Substances Oriented Models

The trust systems in element situated models work at counteracting forever or briefly, noxious elements from transmitting or sending any data. Malicious hubs are repudiated in light of the evaluated notoriety and their past conduct in the system. A large portion of the proposed strategies that are putting forth some level of trust between imparting hubs in specially appointed systems fall inside this class. In [7], the authors proposed an approach utilizing different measurements, for example, situational trust, occasion based trust, dispositional trust , and conviction development trust are proposed to secure interchanges and to save area protection of vehicles. Notwithstanding, it is not clear yet how to make utilization of the diverse blends of these measurements. In [8], the creators present a trust model that protects protection inside shaped gatherings. While offering to safeguard the protection, the plan has two primary weaknesses: First, a security shortcoming is pinpointed for the situation where the gathering pioneer is traded off or when a Distributed Denial of Service (DDoS) assault is propelled by a gathering of malignant hubs. Second, from a consistent perspective, it is difficult to perceive how gathering can be performed in light of substances. When all is said and done, the idea of gathering identifies with having the same geological area more than whatever else. The work in [9] proposes a motivating force show with the capacity to reject pernicious hubs in view of the credit esteem which increments and reductions taking after the conduct of the hub in the system. However, this plan does not consider some trust decencies, for example, circumstance reliance and its distinctive immediate and backhanded measurements [15] [16][17].

2.2 Information Oriented Models

This class of trust models concentrates on checking the information traded amongst hubs and sifting through pernicious messages from continuous correspondences. Nevertheless, methods of this model are construct with respect to the notoriety of hubs and not information itself. For example, the authors of [10] expect that all hubs keep up a model of non-vindictive correspondence that is comprehensively known in the VANET. Every got data is contrasted with this model. On the off chance that hubs gone to a solid assertion about it, then the information will be sent, else, it will be dropped. The principle downside of this approach is the presumption about the worldwide information of this model, which is not achievable in reality. The work in [11] introduce an information based trust demonstrate for ad-hoc fleeting systems where trust between elements is settled also, depends just on the part of elements (e.g. Police vehicles: trust=1, standard vehicles: trust=0.5 ...and so on.) The author utilize Dempster-Shafer hypothesis and Bayesian deduction to assess confirmations with respect to a specific occasion, and utilizing diverse trust measurements keeping in mind the end goal to take a choice about

the level of trust that can be set on the got information speaking to the occasion. The authors additionally propose the utilization of different measurements, for example, undertaking/occasion also, time/area. One of the fundamental disadvantage to this approach is the situation of information sparsity, which would not perform well. Also, having substances bound to a settled trust speak to a disadvantage of this approach realizing that a trust relationship can be dynamic particularly in a very pervasive condition for example, VANET [18][19].

2.3 Half and half trust models

Trust models falling under this classification go for protecting dependable correspondence between hubs in face of unfriendly hubs, which would attempt to exasperate it. So the principle worry of this classification of models is to keep up correspondence and repudiate hubs suspected to intrude on it. As it shows up from the audits of these models in the literature, the principle downside is the inordinate time handling required and in addition, the sum of control messages expected to accomplish this goal. To beat such a debilitate, a structure for messages proliferation furthermore, assessment is proposed in [12]. In this approach, to limit the quantity of traded messages, this plan receives a bunching association, where messages are transferred just between bunch pioneers. After getting a message, a pioneer sends it to the bunch individuals to get their sentiments on this message, at last, in light of the gathered feelings also, the boycott sent by the testament expert (CA), the pioneer can settle on a choice about handing-off the message or not. Be that as it may, this plan adds an essential overhead to messages as it totals confide in feelings and hub marks. It can be considered as wasteful because of choosing a malevolent group pioneer, and gives terrible outcome against double-crossing assaults [20][21].

In [13] a circulated notoriety framework called VARS was proposed, where a companion can create a sentiment about a message in light of the accumulated sentiments of different hubs about it and furthermore utilizing different measurements, for example, immediate and aberrant trust with the sender. So as to give more significance to the conclusions originating from the nearest hubs to the occasion, Dotzer et al. recognize three zones: occasion, choice and dissemination region. The primary weakness of this plan is the overhead included to messages including the other trust hub conclusions. Creators try not to give clear and finish insights about the distinctive strides of their strategy. Moreover it is not disclosed how to bargain with the situation where a malignant hub is the main correspondent as its sentiment will influence every single next supposition. Another bunching trust-based model utilizing subterranean insect settlement directing is proposed in [14]. The bunches are conformed to the RSUs or the slowest and most confided in vehicles. For each message sent by a hub the bunch head accumulates the individual's sentiments on the hub and creates a choice about the message. The subterranean insect settlement calculation is utilized to pick the best way between various bunches utilizing limits hubs. The principle shortcomings of this work are the utilization of a static cluster heads what's more, the ease back sending choice because of the sentiments gathering [22][23].

3 Framework Component

The primary objective of our system is to forestall sending malevolent information in view of self-assessment of the forwarder and the nature of information. Unto the end we present another parameter that consolidates confide in weight of hubs (Tr) and connection steadiness (LS). Keeping in mind the end goal is to pick the most steady and confided in forwarder. Furthermore, disavowing as quick as could reasonably be expected, deceptive hubs from the system. Figure1 modules: Neighboring assessment module, choice module, interchanges module, messages classifier, what's more, an Intrusions Detection Module (IDM). In figure 1 each hub i keeps up a trust an incentive for each single neighbor "j" called Tri , j which is registered utilizing the assessment of the communications with the sender, the sender's part (for example, state autos) and the report of the IDM about sender's conduct. More insights about this weight will be found in the coming areas explored [24][25].

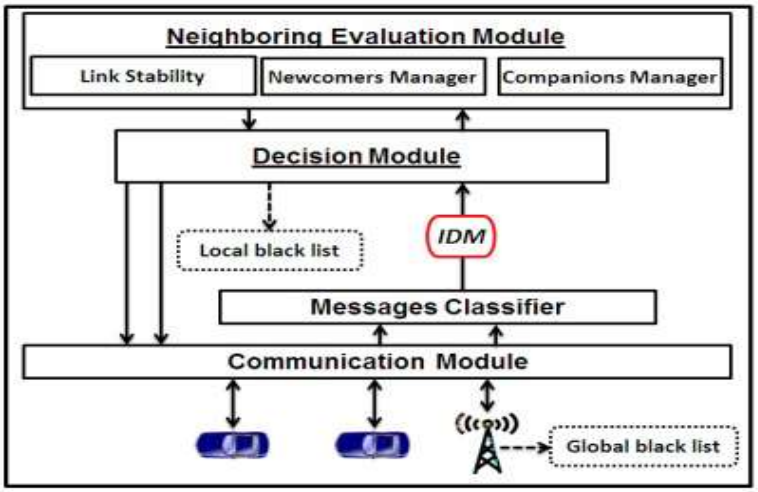


Fig. 1. Framework outline of our plan

3.1 Neighboring Evaluation Module

This module contains three sub-modules dependable for the most part for three errands: (1) processing of connections strength between hubs what's more, its neighbors, (2) overseeing newcomers in the correspondence territory of the hub and (3) explaining the sidekicks list by joining the trust and the connection strength values.

(a) Link Stability Sub-Module: A connection is viewed as steady between two hubs on the off chance that they are neighbors and move generally with a similar speed. To abstain from re-examining a broken connection (e.g. a boisterous channel or a hindrance like a truck) between hubs, we can pick an edge "Th" speaking to the time of "n" reference points, i.e. in the event that the hub "i" surpasses this time without getting a guide from a neighbor hub 'j'. This last is most certainly not considered any more as a neighbor. We compute the connection security esteem LSi; j between two hubs i and j as takes after [26][27].

$$LS_{i,j} = \alpha * LS_{i,j} + (1-\alpha) * \left({}^{1}/_{\rho * \chi}\right) \quad (1)$$

where,

$$\rho = \Delta V_{i,j}(t+\tau)/\Delta V_{i,j}(t) \quad (2)$$

$$\chi = D_{i,j}(t+\tau)/D_{i,j}(t) \quad (3)$$

$$\Delta V_{i,j}(t) = V_i(t) - V_j(t) \quad (4)$$

Here
$V_i(t)$: speed of *i* at time *t*.
$D_{i,j}(t)$: separate amongst *i* and *j* at time *t*.

We utilized α and (1-α) keeping in mind the end goal to maintain a strategic distance from pinnacle cases impact in the general connection related conduct.

(b) Newcomers Sub-Module: This module influences at first to the new neighbors a trust esteem equivalent to 0.5, after co-operation; this esteem can be expanded or diminished after its conduct.

(c) Companions Manager Sub-Module: A friend as known is the individual who invests energy or go with another. In our case, associates are neighbors remaining inside the range of a vehicle for a drawn out stretch of time, which is settled cloister in such approach to permit assessing their practices proficiently. To pick a vehicle as a forwarder, a hub can choose among the associates show a standout amongst the most trusted vehicles that we called TOP mates. This procedure will be re-hashed for each hub to abstain from choosing unscrupulous hubs to coordinate in all transmissions. The top mates are dictated by joining the connection security esteem $LS_{i,j}$ and the trust permitted to them. Along these lines, all neighbors having in the meantime high trust (e.g. 0.6), what's more, high connection security values (LS) can be added to the top associates list.

3.2 Messages Classifier Module

In the standard 802.11p, information movement is separated into four classifications arranged from the most minimal to the most astounding need as takes after: foundation movement (FM), best exertion activity (BE), video activity (VA), and voice movement (VM). Wellbeing messages are out of order on the grounds that a particular band is saved to them. In this work, we embrace the above order with a minor alteration. Thus, we regroup the video activity (VA) in a similar class that we call continuous activity class, and consider the wellbeing messages in a different class as explained in figure 2.

Fig. 2. Classification of information movement.

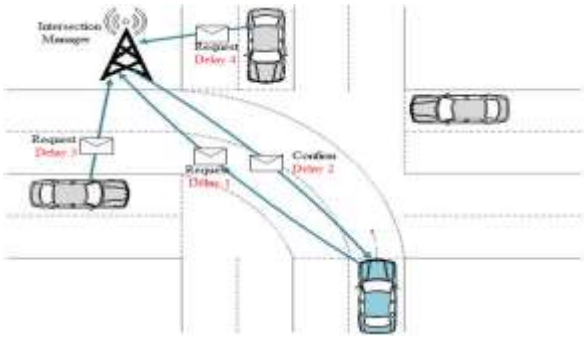


Fig. 3. Interruption Detection Module

3.3 Interruption Detection Module (IDM)

Interruption recognition methods have been customarily characterized into two classes: (i) Misuse recognition that looks in traded bundles a mark of known assaults. (ii) Anomaly discovery where the general conduct of a hub is thought about to a model of anomalous conduct. In our structure, we utilize another interruption identification module that utilizations both abuse and irregularity discovery, and holds for each neighbor a measurable data about sent information.

This can prompt recognize DoS assaults and allow additionally to create a weight W(i) IDM speaking to the genuineness of a sender (or, on the other hand a forwarder). Along these lines, for each neighbor, if a negative activity is monitored by a guard dog strategy as in [16], or its messages sending recurrence surpasses a predefined limit, its weight will be balanced as:

W(i) IDM Attack signature;
W(i) IDM Threshold surpassed;
W(i) IDM W(i) IDM-δ : Negative activity is flagged;
where δ is a decrement-calculate.

At that point, this module can add the hub identifier to a dim list i about a weight, which is not exactly a predefined edge (dangerTh). Additionally, a hub can be privately boycotted if its identifier has a place with the dim rundown and it runs another vindictive activity as shown in Algorithm 1.

Algorithm 1:

```
if W(i) IDM , dangerTh     then
        do some processing
        if Forwarder Destlist     then
                Local list Forwarder
        else
                Destlist Forwarder
        end if
end if
```

The nearby boycott is utilized to avoid as quick as could reasonably be expected, hubs to send or transfer pernicious messages. The denial of such hubs should be possible just for a predefined period, which permits hubs controlling by malignant elements to reintegrate the system operations in the wake of overcoming the security issues. Intermittently, every hub sends its nearby boycott to the RSU which produces a worldwide boycott utilizing neighborhood boycotts. For the long run keeping in mind the end goal to forestall unscrupulous hubs to run a DoS assault, or a spam robot, the general trust of a hub can be refreshed after recognizing a malignant message even after sending it as takes after:

$$T_{r_i'}Forwarder = T_{r_i'}Forwarder + (1-\alpha) * W(i)IDM \quad (5)$$

3.4 Choice Module

This module is the center of our system, it is dependable for settling on a choice about hubs honesties, message quality what is more, forwarder choice. The hub trustworthiness is assessed by consolidating the weights delivered by different modules to compute a trust esteem Tr for each neighbor. So hubs that have a low trust esteem will be rejected from all system operations. The message quality is acquired by hubs utilizing their assessment about the last forwarder and the trust sentiment field piggybacked to each message. So as to have an effective tradeoff between these components, we think about just the assessment of the immediate wellspring of message (forwarder). Clearly on account of no past communications between hubs, malevolent information can be sent since the underlying trust esteem permitting to the hubs don't avoid them to coordinate and furthermore to guarantee conveying bundles in a low end to end delay. By presenting the defer handling, malignant messages can be recognized which prompts drop different messages coming from the same unscrupulous forwarder. The choice procedure utilized as a part of this work is calculated in algorithm 2. For sure, a hub getting a message, checks first its source, in the event that it does not have a place with neighborhood or worldwide boycotts, it ascertains the trust esteem and contrasts it and two limits Thl and Thh speaking as far as possible past which we can consider whether a hub is high or low trusted. Along these lines, if a hub "i" got a message having a trust assessment "T_r" variable=a "from a hub "j" having a trust $T_{r\ (i,j)}$=b then, the new trust assessment that will be related to a bundle.

In the second step, the choice procedure must pick the most satisfactory hub to forward the message, in inclination among Beat friend neighbors, if its feeling that the message surpasses a trust esteem more noteworthy than TrustThToSend, speaking to the least trust, an incentive to forward a message.

γ and δ is increments and decrements factors. We expect additionally that, since companions trust is hard to develop yet simple to tear down [15]. Furthermore, if the punishment calculate (≤1) then they have a place with the dark rundown.

Algorithm 2:

if Sender doesn't belong to Local/Global BLACKLIST **then**
  if Destination is Myid **then**
    Delayed_verification()
  else
    Calculate combined trust of Sender & Message as
    Trust = $T_{me,Sender}$* $Sender_{think}$
  end if
  if Trust ≥ Th_{high} **then**
    My_{think} = $T_{me,Sender}$
  else if
    thenTh_{low} < Trust < Th_{high}
    My_{think} = Avg($T_{me,Sender}$,$Sender_{think}$)
  else
    My_{think} = min($T_{me,Sender}$,$Sender_{think}$)
  end if
  if Sender ∈ My_{Grey_list} **then**
    My_{think} = β*My_{think}
  end if

  if My_{think} ≥ $Trust_{Thresholdtosend}$ **then**
    if Destination ∈ Neighbors **then**
      Send(msg,Myid,My_{think})to Destination
    else
      Send(msg,Myid,My_{think})to BestNextHop
    end if
    $T_{me,Sender}$=$T_{me,Sender}$+0.01
    else
      Drop Message
      $T_{me,Sender}$=$T_{me,Sender}$-0.10

end if
Drop Message-2 =0
end if

---

4 Untrusted hubs location

To assess our trust-based information trade conspire, we have utilized NS-3 arrangement as a test system. To assess our plans adequacy within the sight of a high rate of deceptive hubs, we differed the rate of these deceptive hubs from 10% to 30%. As specified in the Table 1 every hub creates one pernicious message for each 3 seconds rather than 5 seconds as utilized as a part of [12]. Figure 4 demonstrates that the discovery rate increments by expanding the quantity of vehicles in the system.

Clarified by the trust assessment sent by the middle of the road hubs also, the postponed examination guaranteed by the Intrusion Detection Module, which permits distinguishing terrible hubs, and including their identifiers to dim or boycotts.

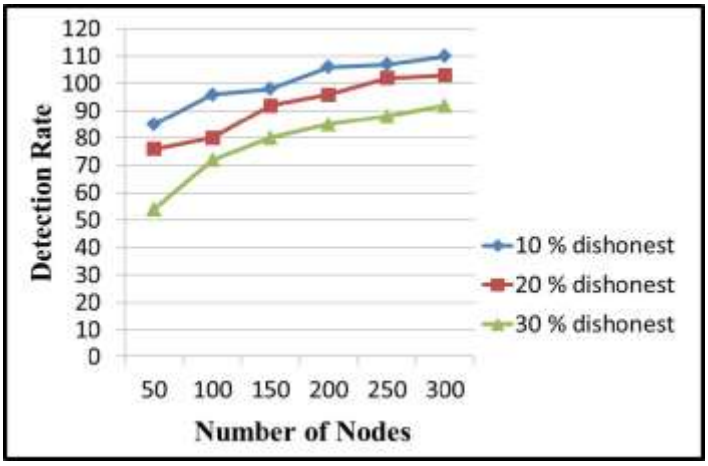


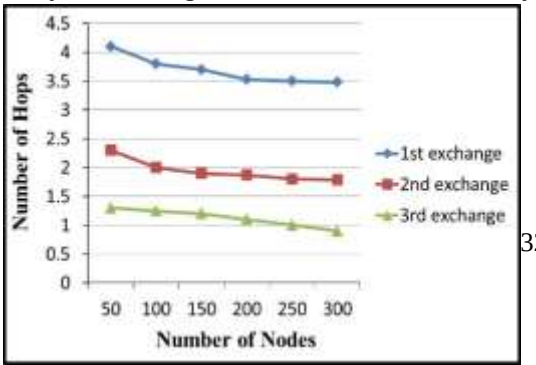
Fig. 3. Dishonest hubs recognition

4.1 The normal number of bounces expected to recognize malevolent information

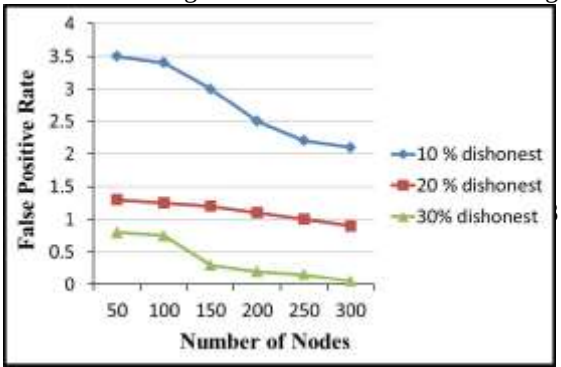
The recognition rate can't give any data about the time expected to boycott terrible hubs. Along these lines, to assess the union as far as number of bounces expected to recognize hubs handing-off negative messages and avert them to send more pernicious information. Figure 5 shows that our plan is forwarding the main message of any new transmission started by new comers in the system. In any case, it meets rapidly and can recognize malevolent information from the primary bounce after the third message sent by the assaults initiator.

4.2 False Positive and False Negative rates

In any security conspire, False Positive (FP) and False Negative (FN) rates are two measurements used to judge its execution. In this manner, for various unscrupulous hubs rate, we process the positive and negative false rates produced by our plan. From Figure 6, unmistakably the FP rate diminishes by expanding the quantity of hubs in the systems, in light of the fact that in a thick system, forwarders have a high likelihood to be chosen among



32-6940



genuine hubs, and on account of a meager organize, legit hubs may hand-off pernicious information sent by distinctive hubs. This can influence their trust and prompts take a false choice about them. With respect to FP, the false negative rate FN relies on upon the organize thickness. In this way, it increments in an inadequate system, and diminishes in the other case. This can be clarified by the reality that an unscrupulous hub can change the following forwarder for each message, which permits to diminish the identification rate and thusly builds the FN rate.

Fig. 4. Average number of bounces expected to recognize malignant information.

Fig. 5. False Positive of unscrupulous hubs discovery.

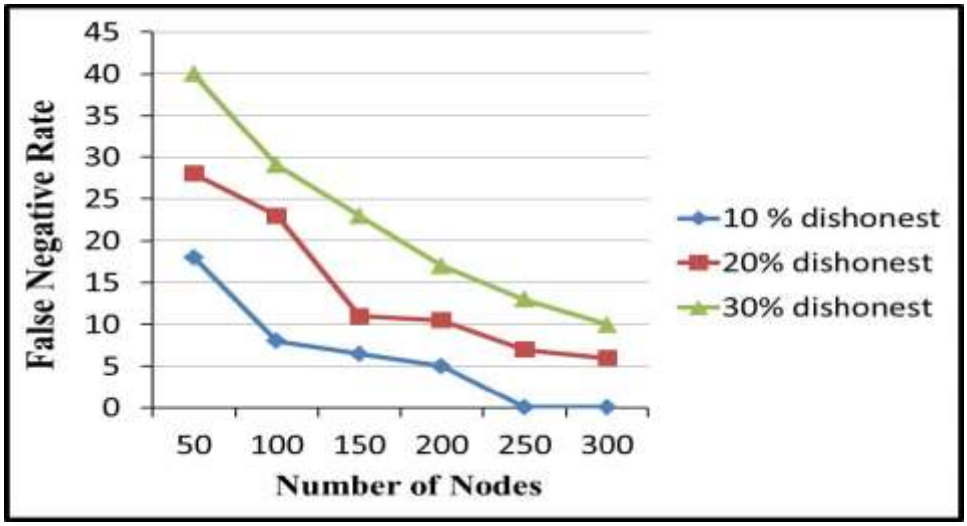


Fig. 6. False Negative of unscrupulous hubs discovery

5 Conclusion

In this paper, we exhibited another trust methodology, who's points at upgrading and securing the message transfer system in VANETs. We presented a deferred message-check approach, which permits message transferring to be facilitated while assessing, and assembling a feeling about neighboring hubs and getting messages is continuous. We consolidated in this approach, an interruption recognition module (IRM) which is in charge of enhancing the trust processing. The trust assessment calculations with IRM makes additionally utilization of the idea of friend hubs so to keep away from correspondence through hubs with plausible deceptive nature. To give more power to our methodology, we utilized distinctive trust measurements, for example, trust values issued from the part based vehicles, and the trust feelings included to the message by each moderate hub before sending it to the receiver. Results have portrayed that our methodology can reach a high discovery rate of unscrupulous hubs in the system even because of DoS assault. As future works, we plan to add different measurements to our approach to accomplish more power and better exhibitions as far as low false positive and negative rates. We arrange moreover to adjust an urban steering methodology for our plan.

6 References

1. C. V. N. Index, "Global mobile data traffic forecast update, 2016–2021 white paper," 2017.
2. A. Ghodsi, S. Shenker, T. Koponen, A. Singla, B. Raghavan, and J. Wilcox, "Information-centric networking: seeing the forest for the trees," in Proceedings of the 10th ACM Workshop on Hot Topics in Networks. ACM, 2011, p. 1.
3. T. Koponen, M. Chawla, B.-G. Chun, A. Ermolinskiy, K. H. Kim, S. Shenker, and I. Stoica, "A data-oriented (and beyond) network architecture," in ACM SIGCOMM Computer Communication Review, vol. 37, no. 4. ACM, 2007, pp. 181–192.
4. F. R. Salguero, "Content mediator architecture for content-aware networks," COMET EU FP7 Report, 2010.
5. V. Jacobson, M. Mosko, D. Smetters, and J. Garcia-Luna-Aceves, "Content centric networking," whitepaper 2007, 2009.

6. L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, P. Crowley, C. Papadopoulos, L. Wang, B. Zhang et al., "Named data networking," ACM SIGCOMM Computer Communication Review, vol. 44, no. 3, pp. 66–73, 2014.
7. L. Zhang, D. Estrin, J. Burke, V. Jacobson, J. D. Thornton, D. K. Smetters, B. Zhang, G. Tsudik, D. Massey, C. Papadopoulos et al., "Named data networking (ndn) project," Relatório Técnico NDN-0001, Xerox Palo Alto Research Center-PARC, 2010.
8. V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking named content," in Proceedings of the 5th international conference on Emerging networking experiments and technologies. ACM, 2009, pp. 1–12.
9. A. Compagno, M. Conti, P. Gasti, and G. Tsudik, "Ndn interest flooding attacks and countermeasures," in Annual Computer Security Applications Conference, 2012.
10. P. Gasti, G. Tsudik, E. Uzun, and L. Zhang, "Dos and ddos in named data networking," in 2013 22nd International Conference on Computer Communication and Networks (ICCCN), July 2013, pp. 1–7.
11. A. Afanasyev, P. Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang, "Interest flooding attack and countermeasures in named data networking," in IFIP Networking Conference, 2013. IEEE, 2013, pp. 1–9.
12. K. Wang, H. Zhou, Y. Qin, and H. Zhang, "Cooperative-filter: countering interest flooding attacks in named data networking," Soft Computing, vol. 18, no. 9, pp. 1803–1813, 2014.
13. H. Dai, Y. Wang, J. Fan, and B. Liu, "Mitigate ddos attacks in ndn by interest traceback," in Computer Communications Workshops (INFOCOM WKSHPS), 2013 IEEE Conference on. IEEE, 2013, pp. 381–386.
14. K. Wang, H. Zhou, Y. Qin, J. Chen, and H. Zhang, "Decoupling malicious interests from pending interest table to mitigate interest flooding attacks," in Globecom Workshops (GC Wkshps), 2013 IEEE. IEEE, 2013, pp. 963–968.
15. A. Afanasyev, I. Moiseenko, L. Zhang et al., "ndnsim: Ndn simulator for ns-3," University of California, Los Angeles, Tech. Rep, 2012.
16. Kumar, Vimal, and Rakesh Kumar. "An adaptive approach for detection of blackhole attack in mobile ad hoc network." Procedia Computer Science 48 (2015): 472-479.
17. Kumar, Vimal, and Rakesh Kumar. "Detection of phishing attack using visual cryptography in ad hoc network." 2015 International Conference on Communications and Signal Processing (ICCSP). IEEE, 2015.
18. Kumar, Vimal, and Rakesh Kumar. "An optimal authentication protocol using certificateless ID-based signature in MANET." Security in Computing and Communications: Third International Symposium, SSCC 2015, Kochi, India, August 10-13, 2015. Proceedings 3. Springer International Publishing, 2015.
19. Kumar, Vimal, and Rakesh Kumar. "A cooperative black hole node detection and mitigation approach for MANETs." Innovative Security Solutions for Information Technology and Communications: 8th International Conference, SECITC 2015, Bucharest, Romania, June 11-12, 2015. Revised Selected Papers 8. Springer International Publishing, 2015.
20. Kumar, Vimal, et al. "Prevention of Blackhole Attack in MANET using Certificateless Signature Scheme." Journal of Scientific & Industrial Research 81.10 (2022): 1061-1072.
21. Deshwal, Vaishali, and Vimal Kumar. "Study of Coronavirus Disease (COVID-19) Outbreak in India." The Open Nursing Journal 15, no. 1 (2021).
22. Narayan, Vipul, et al. "Enhance-Net: An Approach to Boost the Performance of Deep Learning Model Based on Real-Time Medical Images." Journal of Sensors 2023 (2023).
23. Babu, S. Z., et al. "Abridgement of Business Data Drilling with the Natural Selection and Recasting Breakthrough: Drill Data With GA." Authors Profile Tarun Danti Dey is doing Bachelor in LAW from Chittagong Independent University, Bangladesh. Her research discipline is business intelligence, LAW, and Computational thinking. She has done 3 (2020).
24. Faiz, Mohammad, et al. "IMPROVED HOMOMORPHIC ENCRYPTION FOR SECURITY IN CLOUD USING PARTICLE SWARM OPTIMIZATION." Journal of Pharmaceutical Negative Results (2022): 4761-4771.
25. Narayan, Vipul, A. K. Daniel, and Pooja Chaturvedi. "E-FEERP: Enhanced Fuzzy based Energy Efficient Routing Protocol for Wireless Sensor Network." Wireless Personal Communications (2023): 1-28.
26. Tyagi, Lalit Kumar, et al. "Energy Efficient Routing Protocol Using Next Cluster Head Selection Process In Two-Level Hierarchy For Wireless Sensor Network." Journal of Pharmaceutical Negative Results (2023): 665-676.
27. Paricherla, Mutyalaiah, et al. "Towards Development of Machine Learning Framework for Enhancing Security in Internet of Things." Security and Communication Networks 2022 (2022).