INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

(Volume2, Issue3)

Available online at: www.Ijariit.com

SECURE AUTHENTICATION BASED TRUST EVALUATION IN VANETS

Meenu Setia[1], Mrs. Parul Dua[2]

Student[1], Associate Professor[2]

Department Of Computer Science and Engineering, DIET, Karnal

Haryana-132001

Abstract— Trust and its association are thrilling fields of research. The affluent works producing concerning belief gives us a forceful indication that this is a vital span of research. Belief as a believed has an expansive collection of adaptations and requests, that reasons divergence in belief association terminology. The aim of this paper is to furnish VANETs designers alongside several perspectives on the believed of belief, an understanding of the properties that ought to be believed in growing a belief metric, and visions on how belief can be computed. We commenced this paper by giving assorted definitions of belief and metrics utilized for assessing trust. We next gave a comprehensive survey of assorted belief computing ways, their comparisons alongside respect to assorted attack models and computational requirements. We analyzed assorted literatures on the belief dynamics such as belief propagation, aggregation and predictions. In the end we have endowed a serving detailing the request of belief mechanisms in security. The belief schemes gave in this discover cover an expansive scope of request and are established on countless disparate kinds of mechanisms. There is no solitary resolution that will be suitable in all contexts and applications. As arranging a new belief arrangement, it is vital to ponder the constraints and the kind of data that can be utilized as input by the network. A finished observation is that so distant, the continuing scrutiny work and propositions lack completeness. There are vital subjects yet to be addressed.

Keywords: Vehicular Ad hoc Networks, Sybil Attacks, Position Verification

I. WHAT IS VANET

VANET [1] is the knowledge of constructing a robust Ad-Hoc web amid mobile vehicles and every single supplementary, as well, amid mobile vehicles and roadside units. As shown in Fig. 1-1, there are two kinds of nodes in VANETs; mobile nodes as On Board Units (OBUs) and static nodes as Road Side Constituents (RSUs). An OBU resembles the mobile network module and a central processing constituent for on-board sensors and notice devices. The RSUs can be climbed in centralized locations such as intersections, parking lots or gas stations. They can frolic a momentous act in countless requests such as a gate to the Internet. The frank construction of VANET is shown in figure 1.2. VANET presents a new and enthusing earth of scrutiny, progress and standardization. Throughout the globe, there are countless nationwide and global undertakings in governments, industry, and academia devoted to the progress of VANET protocols.

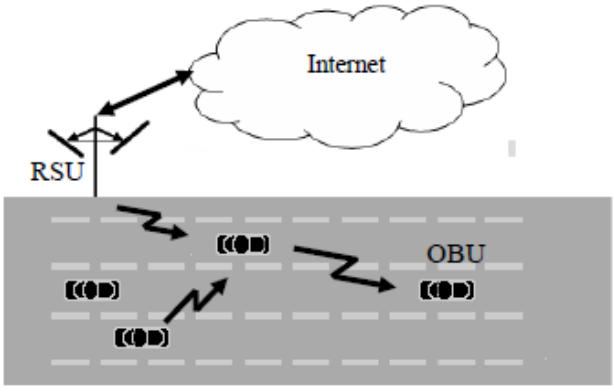


Fig. 1.1. Node types in VANETs

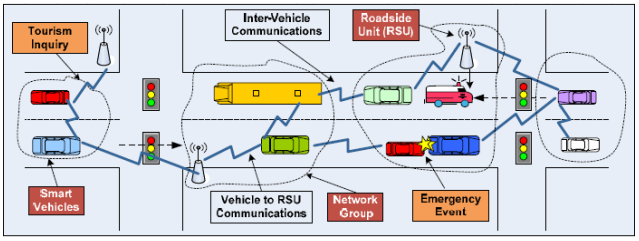


Figure 1.2: Basic structure of VANET

These projects include consortiums like 'The Dedicated Short Range Communications(DSRC)' (USA), the 'Car-to-Car Communication' (Europe) and the 'Intelligent Transportation Systems ' (Japan), and standardization efforts like the IEEE 802.11p'Wireless Access in Vehicular Environment' (WAVE).

II. WHY VANET

The Bureau of Transportation Statistics described that, in 2004 inside the USA only, there were extra than 6.4 million kilometers of freeway, alongside extra than 243 million registered vehicles of disparate kinds running across them. Across that year, there were more than 6.18 million vehicle crashes provoking concerning 2.79 million injuries and 42,000fatalities. Car accidents are the managing cause of demise in the period cluster of 1 to 44 years [35].These accidents price extra than $150 billion each year [11]. With these magnificent numbers, considerable governmental and supplementary connected agencies' as well as investments of vehicles manufacturers have been there trying to protection of roads.

Accordingly, vehicle manufacturers are contesting in equipping their vehicles alongside devices that amass data from the inside and exterior of vehicles and hold it to a central processing unit that can examine this data to boost the road protection as rising the on-board luxury. Global positioning arrangements (GPS), Event Data Record (EDR) resembling the Black-Box used in avionics, tiny scope radars, evening vision, light sensors, rain sensors and navigation systems are well-known intelligent mechanisms utilized in countless presently produced vehicles, what is rather denoted to as "Computers-on-Wheels". Communication researchers have been presently working on a prominent step; if each vehicle has a mechanism that can converse alongside supplementary vehicles, vehicles will have a gigantic new basis of data that extends beyond the skills of all beforehand mentioned devices. For example, all of these mechanisms cannot alert the driver of a halting vehicle in the next coil and of sequence cannot allow travelers relish video chatting and file allocating at no charge. Moreover, alongside this knowledge, vehicles can converse to every single supplementary and notify every single supplementary of any probable danger and could even answer to that danger in a obliging manner, i.e., introducing what could be rather denoted to as "Computer Networks-on-Wheels".

Under heavy manufacturing pressure, it is seeming that VANETs are probable to come to be the most relevant realization of mobile Ad-Hoc networks. Motivations of the enthusing VANET technology contain but are not manipulated to,

1 Increase traveler safety
2 Enhance traveler mobility

3 Decrease travelling time
4 Conserve energy and protect the environment
5 Magnify transportation system efficiency
6 Boost on-board luxury

Related governmental authorities are expected to set a number of new rules and regulations forcing all vehicle manufacturers to equip their vehicles with VANET transceivers employing some of the required safety applications.

III. SYBIL ATTACK

The peer-to-peer (P2P) paradigm of computing has a lot of gains above supplementary standard paradigms. For example, in this paradigm, resources such as bandwidth, recollection, and data are made obtainable to supplementary all giving users [1]. Broadly, this paradigm includes structured and unstructured systems. Structured overlays, such as Kademlia [2] and Chord [3], furnish deterministic mechanisms for data and peer invention, whereas unstructured overlays, such as Gnutella [4], coordinate peers in a random graph and use flooding for peers and data discovery. Most of the accepted peer-to-peer arrangements lack centralized powers that makes this paradigm robust opposing wreck attacks. On the supplementary hand, the lack of such centralized powers leads to countless challenging protection issues; most services vital for safeguarding networked arrangements need one kind of centralized power or one more, making these services unavailable to peer-to-peer arrangements [5]. Even inferior, the fully decentralized and open nature of countless of these arrangements enables a expansive scope of protection menaces unfamiliar in supplementary distributed arrangements, encompassing the Sybil attack [6].

The Sybil attack is well recognized in the context of peer-to-peer, wired, and wireless networks. In its frank form, a peer representing the attacker generates as countless individualities as she can and deeds as if she is several peers in the arrangement [6] aiming at interjecting the normal deeds of the system. The number of individualities that an attacker can produce depends merely on the attacker's skills, that are manipulated by the bandwidth needed for responding to concurrent demands by supplementary peers in the arrangement, the recollection needed for storing routing data of supplementary peers corresponding to every single and every single generated Sybil individuality, and computation resources needed for assisting concurrent demands lacking noticeable delay. With sharp hardware development (e.g., in words of storage capacity and processing power) as well as the range of broadband Internet alongside elevated bandwidth rates, even attackers running on ―commodity‖ hardware can cause comprehensive damage to colossal systems.

The attack itself is accepted and competent in countless contexts and on services that are vital in peer-to-peer arrangements as well as supplementary generic distributed arrangements and paradigms. Such contexts contain electing arrangements, standing arrangements, routing, and distributed storage, amid others. To illuminate how this attack works in real arrangements, envision a recommender arrangement crafted above a peer-to-peer overlay [7]. In such a arrangement, the aim is to filter data that is probable to be of attention to users established on others' recommendations. In that context, an attacker who can deed as several users by faking several individualities can facilely out-vote legitimate users' votes on legitimate objects that are subjected to voting. This is nearly guaranteed, given that the number of legitimate users who normally poll is always no extra than 1% of the finished number of users in each realistic recommendation arrangement [7]. Such an attack becomes appealing to possible users trying to seize supremacy of an arrangement that provides incentives. For example, countless online marketplaces, such as eBay, use recommendations from clients to ascertain the standing of the people who use the period to vend goods, and therefore there is an incentive for such sellers to gain a larger reputation. The alike scenario arises in countless supplementary contexts, such as peer-to-peer file allocating whereas content is rated by users, whereas bandwidth is allocated established on standing, or after standing is utilized to ascertain the worth of content distributed by users. In all such examples, users have an incentive to seize unfair supremacy, and the Sybil attack has proven an influential instrument for attackers to accomplish such goals.

To protect opposing the attack, there have been countless endeavors in the form of armaments, or mitigations, to protect opposing, or check, the encounter of the attack. Such endeavors can be categorized mainly into two schools of thoughts: centralized and decentralized (i.e., distributed) defenses. In centralized armaments [6, 8-10], a centralized power is accountable for verifying the individuality of every single and every single user in the system. As this protection is somewhat competent in protecting opposing the attack, it makes precise assumptions concerning the arrangement, a little of that are not facile to accomplish in peer-to-peer decentralized systems. Early of all, as the term and description implies, such arrangements need a centralized power that could not be affordable for both protection and functionality reasons. Even if such a centralized power exists, it needs credentials for users in

the arrangement to match opposing every single user's digital identity. In countless settings, obtaining such credentials is extremely challenging.

On the supplementary hand, countless decentralized armaments [7, 11-16] do not need such powers and are well projected for decentralized peer-to-peer systems. At the core of their procedure, such armaments weigh collaboration amid users in the arrangement to confess or refuse users who are possible attackers. Admission or rejection of users is established on credentials associated alongside them, as in the case of cryptographic distributed armaments, or web properties of legitimate, candid users, as in the case of Sybil armaments employing communal graphs. In whichever of these resolutions, the ultimate aim of the protection is to simulate the manipulation of the centralized power in a decentralized manner and use such manipulation to notice both Sybil and candid nodes.

Another association of protection might be according to the method the protection operates. Accordingly, continuing armaments in the works can be categorized into those employing 1) trusted certification—in that certificates are normally generated for candid users and confirmed opposing an area key of a trusted power, 2) incurring cost—in that users are penalized in a method that limits their obtainable resources and therefore reduces each misbehavior, and 3) communal network–based Sybil defenses.

These armaments differ considerably in their assumptions, in the kind of web they are requested to, in the guarantees they furnish, and in the prices incurred. Briefly it can be said that node illegitimately claims several individualities or claims fake IDs, the WSN suffers from an attack shouted Sybil attack. The node replicates itself to make countless duplicates to mystery and downfall the network. The arrangement can attack inside or externally. External aggressions can be stopped by authentication but not the inner attacks. There ought to be one to one mapping amid individuality and entity in WSN. But this attack violates this one-to-one mapping by crafting several individualities [6].

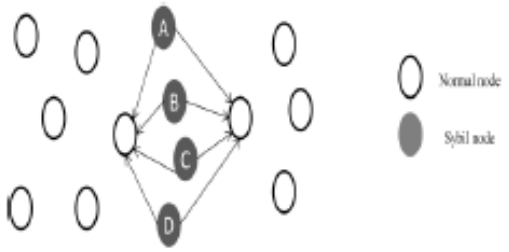


Fig-1.3 Sybil Attack

In fig 3.1 A, B, C, D is the Sybil nodes. When these nodes want to communicate to their neighboring nodes they use any one of the identities. This confuses and collapses the network.

IV. TYPES OF SYBIL ATTACK

In order to detect the Sybil attack it is necessary to understand the different forms in which the network is attacked [1].

(a) Direct and Indirect Communication:

In direct attack, the legitimate nodes communicate directly with Sybil nodes whereas in indirect attack, the communication is done through malicious node.

(b) Fabricated and stolen identities:

It creates a new identity for itself based on the identities of the legitimate nodes, that is, if legitimate nodes have an ID with length 32 bit integer, it randomly creates ID of 32 bit integer. These nodes have fabricated identities.

In stolen identities, attacker identifies legitimate identities and then uses it. The attack may go unidentified if the node whose identity has been stolen is destroyed. Identity replication is when the same identities are used many times in the same places.

(c) Simultaneous and non-simultaneous attack:

In simultaneous, all the Sybil identities participate in the network at the same time. Since only one identity appears at a time, practically cycling through identities will make it appear simultaneous.

The number of identities the attacker uses is equal to the number of physical devices; each device presents different identities at different times.

Sybil attack on protocols

In a Sybil attack, a malicious node can produce and manipulation a colossal number of individualities on a solitary physical device. This gives the illusion to the web as if it were disparate legitimate nodes. It can alter the pursuing vital protocol [1]:

Distributed Storage the Sybil attack affects the design whereas it replicates the data on countless nodes. Data will be stored on Sybil identities.

Routing: Routing mechanism, in that the nodes are hypothetical to be disjoint, is altered by Sybil individualities because one node will be present in the assorted trails and disparate locations at the alike time.

Data Aggregation: In sensor webs, data is gathered into one node to form finished information. After a Sybil node contributes countless periods acting as disparate users, the aggregated data adjustments completely therefore providing fake information.

Voting: In WSN, most of the decisions are made by voting. As the Sybil node has countless individualities, a solitary node has a chance of electing countless periods, therefore destructing the process.

Misbehavior detection: A Sybil node increases the standing, trust, and belief worth by employing its adjacent identities. Therefore the accuracy to notice a malicious node is reduced.

Fair resource allocation: As the Sybil node has several individualities it affects the allocation of resources. For example, after countless nodes allocate a solitary wireless channel, every single node will be allocated a fraction of period each interval across that they can transmit. As the Sybil node has countless individualities, it can attain an unfair allocate of the resources therefore cutting the actual allocate of resources to the legitimate node.

V. WHAT IS TRUST?

The believed of belief is vital to contact and web protocol designers whereas instituting belief connections amid giving nodes is critical to enabling cooperative optimization of arrangement metrics. Belief is described as "a set of relations amid entities that give in a protocol. These relations are established on the facts generated by the preceding contact of entities inside a protocol. In finish, if the contact have been devoted to the protocol, next belief will amass amid these entities .According to, Belief has additionally been described as the degree of belief concerning the deeds of supplementary entities (or agents)

VI. CONCEPTS AND PROPERTIES OF TRUST

In this section, we review how trust is defined in different disciplines and how these trust concepts can be applied in modeling trust in VANETs. Further, we examine the relationship between trust and risk, and how trust should be defined in order to realistically reflect the unique characteristics of VANETs.

A. Multidisciplinary Concept of Trust

According to Merriam Webster's Dictionary, belief is described as assured reliance on the character, skill, strength, or truth of someone or something." Although the subjective nature of belief, the believed of belief has been extremely appealing to web protection protocol designers because of its varied applicability as a decision making mechanism. We scrutinize the works to discover how belief is described in assorted disciplines encompassing sociology, economics, philosophy, psychology, organizational association, and autonomic computing in manufacturing and arrangement engineering. Finally, we additionally scrutinize how belief can be described in contact and networking alongside the aid of definitions in supplementary fields.

Trust in sociology: Gambetta's believed of belief is popularly shouted sociological belief and is described as an assessor's a priori subjective probability that a person (or agent, or group) will present specific deeds that alter the assessor. That is, Gambetta describes the nature of belief as subjectivity, an indicator for upcoming deeds, and dynamicity established on constant contact amid two entities. Luhmann additionally emphasized the significance of belief in area as a mechanism for constructing cooperation amid people to spread human contact for upcoming collaboration. Adams et al. rephrased Gambetta's belief believed in requesting the sociological believed of belief in computer science; they embodied belief as a constant variable, quantifying belief in the light of context or agreement of risk. They more stressed that endangering betrayal is an vital aspect in constructing trust. To be functional, web belief models have to arrest this subjective aspect of communal trust.

Trust in economics: Economists discriminate amid the confidential, casual belief that comes from being approachable alongside your acquaintances and the impersonal, institutionalized belief that lets you give your trust card number out above the Internet. Both notions of belief are vital in martial VANETs. In economics, belief is embodied as an anticipation that applies to situations in that trustors seize risky deeds below uncertainty or data incompleteness. Though, as illustrated in the Prisoner's Dilemma (PD)

game, belief in economics is established on the assumption that humans are rational and severe utility maximizers of their own attention or incentives. In this sense, after we apply a human belief ideal to a web belief ideal, the assumption of egocentric nodes seems reasonable. But altruistic behaviors can appear from mechanisms that could be primarily exclusively egocentric, and therefore making an argument for redemption mechanisms. Commercial models are utilized in conjunction alongside trust-based encryption primitives in to develop a belief association paradigm for safeguarding data flows across organizations.

Trust in philosophy: According to the Stanford Cyclopedia of Philosophy, belief is vital but dangerous. As belief permits us to form connections alongside others and to rely on others for love, counsel, aid, etc., belief is considered as an extremely vital factor in our existence that compels others to give us such things alongside no beyond power such as the law. On the supplementary hand, as belief needs seizing a chance that the trustee could not behave as the trustor expects, belief is hazardous implying the probable betrayal of trust. In his comments on Lagerspetz's book shouted Trust: The Unspoken Demand, Lahno describes the author's think on belief as an ethical connection in human society. Lagerspetz's trusts that investigations of belief expose that human people, their beliefs, desires and deeds are merely intelligible opposing the background of continuing communal habits and communal ties". This implies that reliant on the nature of confidential connections amid a trustor and a trustee (i.e., ethical connection amid them), trustful deeds or betrayal can occur.

Trust in psychology: According to the Wikipedia meaning of belief in psychology [25], belief starts from the origin of the child. As the youngster grows older, belief additionally grows stronger. Though, the origin of belief derives from the connection amid mother (or caregiver) of the youngster as the strength of the relations relies on belief, if the youngster is increased in a relations that is extremely consenting and loving, the youngster additionally returns those feelings to others by trusting them. But if belief is capitulated, it is hard to recover it. In this sense, belief in psychology emphasizes the cognitive procedure that human beings discover belief from their experiences. Deutsch defines belief as the assurance that one will find what is wanted from one more rather than what is feared. An individual could be said to have belief in the occurrence of an event if he expects its occurrence and his anticipation leads to the deeds that he perceives to have larger negative aftermath if the anticipation is not confirmed than affirmative aftermath if it is confirmed. In supplement, Hardinand Rotter noted in their examinations that past experience could strikingly alter afterward capacity for trust. For example, bad experience alongside people will lower the belief level, managing to less trusted connections alongside people, and therefore less opportunities for public gain. Further, they understood that the gains obtained by possessing elevated belief connections exceed the defeat by possessing low belief relationships. For instance, elevated trustors are less probable to lie or mislead or steal. Additionally they are less probable to be unhappy, conflicted, or precarious, and pursued by extra friends. Even nevertheless elevated trustors are misled extra frequently in novel situations, low trustors are additionally fooled equally by distrusting trustworthy people, thereby losing the gains that elevated trustors could have.

Trust in organizational management: In this earth, the believed of belief is additionally described as the extent to that one party is keen to count on someone or something alongside a feeling of comparative protection in spite of probable negative aftermath, emphasizing the potential of confronting risk. Schoorman et al.defined belief as the willingness to seize a chance or willingness to be vulnerable in the connection in words of skill, integrity, and benevolence. They additionally clarified that belief is not vitally public and is not reciprocal. Belief thoughts in organizational association can give us visions on how to compute belief by investigating methods to compute skill, integrity, and benevolence of every single networked node, as well as on assessing risk. They can additionally give us visions on delineating cluster belief (i.e., amid a person and a cluster or amid groups) that is vital for vibrant areas of interest.

Trust in autonomic computing: As knowledge becomes extra convoluted, fully understanding automation becomes impossible, if not impossible, and belief in automation becomes critical, chiefly after unexpected situations arise and arrangement replies cannot be predicted. Researchers studying autonomic computing in manufacturing arrangements engineering have pursued to develop models of belief to comprehend how belief in automation develops and how it could be misplaced. Lee and Observe delineate belief as the attitude that an agent will aid finish an individual's aims in a situation alongside uncertainty and vulnerability. In this sense, an agent can be automation or one more person that actively interacts alongside the nature on behalf of the person. Parasuraman links the level of belief alongside automation reliability uttering that. Trust frequently determines automation usage. Operators could not use a reliable automated arrangement if they trust it to be untrustworthy." The believed of automation reliability as a belief metric is one that is applicable in VANETs, whereas the user's belief in reliability on knowledge is an vital aspect. Belief in contact and networking: The believed of belief additionally has been appealing to contact and web protocol designers whereas belief connections amid giving nodes are critical in constructing obliging and cooperative settings to optimize arrangement goals in words of scalability, configurability, and reliability (i.e., survivability), dependability, or security. According to Eschenauer et

al., belief is described as a set of relations amid entities that give in a protocol. These relations are established on the facts generated by the preceding contact of entities inside a protocol. In finish, if the contact have been devoted to the protocol, next belief will amass amid these entities." Capra proposes to use a human belief ideal established on human contact in a belief ideal for fully distributed web settings such as VANETs. Capra defines belief as the degree of a belief concerning the deeds of supplementary entities (or agents). Li and Singhal delineate belief as the belief that an entity is capable of giving reliably, dependably, and securely in a particular case; hence, disparate levels of belief continue in disparate contexts. For example, Alice could belief her physician to give her counsel on her condition concerns but could not belief her physician's counsel on fixing her car.

Recently, researchers have understood the significance of communal webs in constructing belief connections amid entities. Golbeck introduces the believed of communal belief by counseling the use of communal webs as a connection to craft belief connections amid entities. Golbeck proposes the request of a belief believed derived from a sociological

Proposed Flow chart

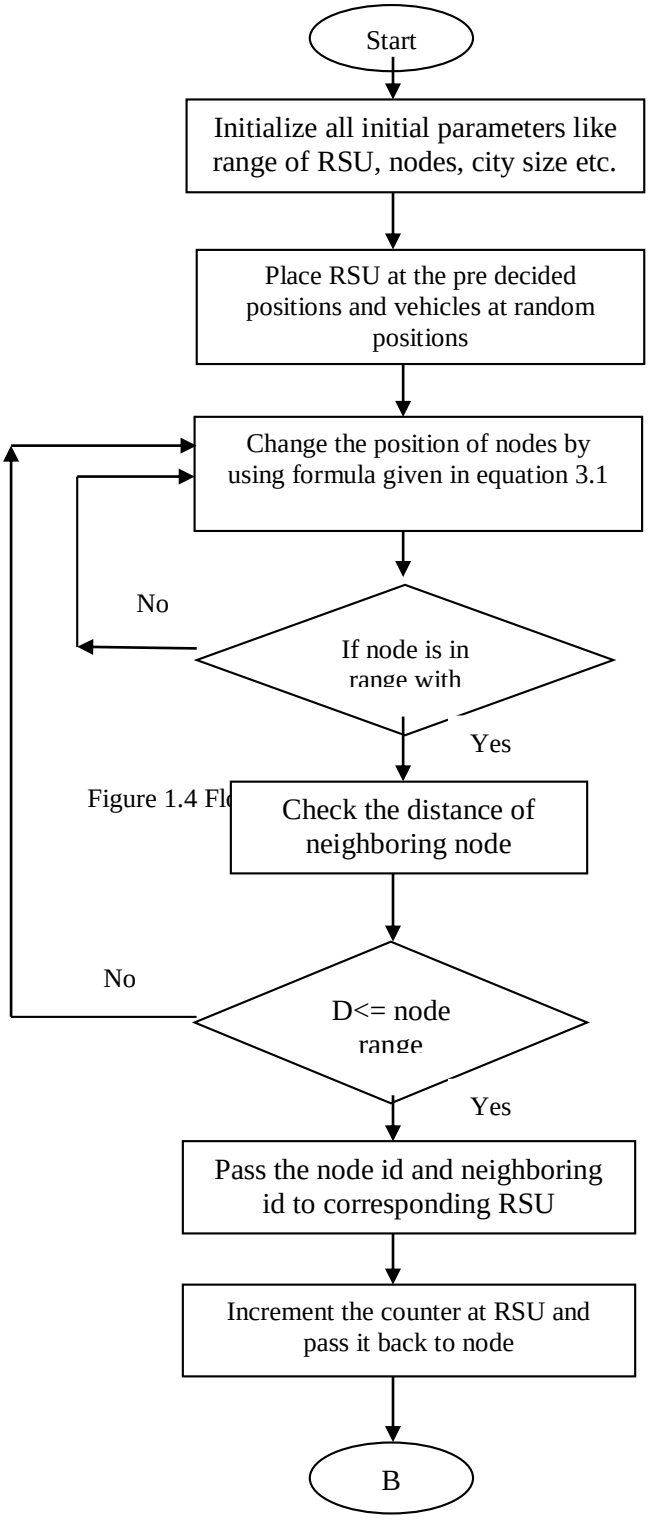
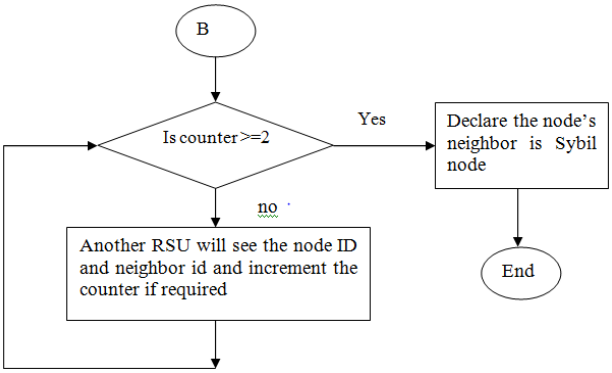


Figure 1.4 Fl



VII. RESULTS AND ANALYSIS

In this simulation even though 5 Sybil nodes are allocated but as they are advancing randomly and they have to cross at least two RSU to be noticed as Sybil node, so there is potential that Sybil node moves out of metropolis beforehand crossing two RSU or the node that is chased by Sybil node change its path. In that case that Sybil node will not be noticed by RSU as Sybil node. This potential can be evaded if metropolis blocks are increased and scope of RSU is decreased. For a moment the table 1 displays the id Sybil nodes allocated alongside the nodes and id of RSU s across that those nodes bypassed.

Table 1: Sybil node's neighboring node id and corresponding RSU's id

Sybil nodes position	75	18	58	6	59

RSU ID	Node ID
1472016	65
1472026	71
1472026	69
1472027	75
1472031	71
1472031	71
1472032	18
1472036	71
1472046	18
1472047	48
1472047	75
1472048	57
1472048	57
1472048	78
1472050	71
1472050	69
1472050	20
1472051	18
1472051	79
1472053	57
1472055	71
1472057	75
1472058	57
1472060	71
1472062	1
1472063	57

Above table shows the node IDs which are followed by Sybil nodes. On analyzing the table it has been noted that the RSU id is changing as well as node id but some node ids repeat themselves. So these node ids which are moving through different RSUs will be considered and a counter will be started which will be incremented every time when the same node iD pass through different RSU. Table 5.3 shows the counter value for targeted node id.

Counter	Node ID
1	1
1	20
1	48
1	65
1	78
1	79
2	69
3	18
3	75
5	57
7	71

Table 5.3: Counter for respective node ID

From above table the node possessing counter worth extra than 2 or equal to 2 will be believed as the possible node that is pursued by Sybil node that is highlighted in above table. So, 5 IDs are pursued by Sybil nodes. But the id no. 71 was not allocated the id to that Sybil node follows, so it is fake noticed node id. So it can be said that out of 5 sybil nodes, 4 nodes have been noticed accurately alongside one fake detection. If number of Sybil nodes is modified next additionally our algorithm is able to notice nodes. Below table proves this alongside statistics and figure 5.5 displays that into graphical representation for extra vision understanding. Figure 5.5(a) assesses the correct credit rate alongside the number of actual Sybil nodes in the web and figure 5.5(b) displays the analogy of percentage of correct Sybil node detection alongside the number of nodes. Form bar graph it is clear that after Sybil nodes were 5, next correct detection percentage is highest. The statistics could change in subsequent period simulation as random locations of nodes are utilized every single period.

Table 5.4: comparison table for Sybil node detection w.r.t. various number of Sybil nodes

Number of Sybil nodes	Sybil nodes detected	False detection	Correct Detection (%)
5	4	1	80
10	6	4	60
15	10	5	66.6
20	14	6	70
25	17	8	68
30	22	8	73.3

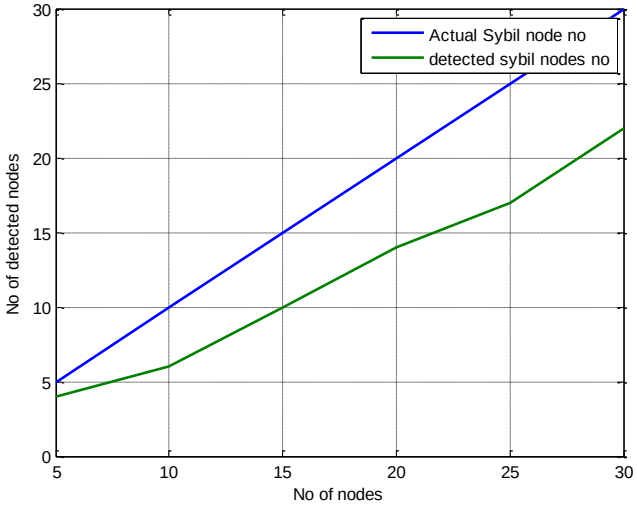


Figure 5.5(a): Comparison of correct detection of Sybil nodes with total Sybil nodes

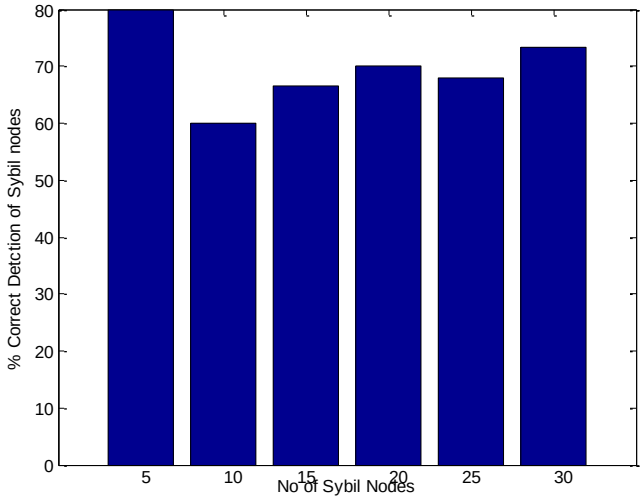


Figure 5.5(b): bar chart for % correct detection of sybil nodes

VIII. CONCLUSION AND FUTURE SCOPE

In this thesis we concentrated on the progress of protection mechanisms to prevent the Sybil attack in wireless ad hoc networks. The cornerstone of our work are resource examinations, a promising technique that permits the mitigation of sybil individualities, lacking needing each pre-configuration of the nodes, being therefore able of enhancing the scalability of the network. We have utilized here the resource assessing method. In this bordering data by vehicles is transferred to road side constituents at a price extremely less overhead in transmission and rest work lies alongside RSU not alongside vehicle. RSU adds a counter to data traversed back to vehicle so that supplementary RSU can check the preceding data of vehicle. This data helps RSU to recognize the Sybil node. In upcoming work this algorithm can be tested for ad hoc webs also. We have consented that power of every single node is alike but this is not the case of useful life. So pondering the power consumption into simulation, algorithm can be extra approaching to real examples. Yet there is colossal number of fake detections in case of extra blocks in the city. Algorithm can be adjusted for this.

IX. REFERENCES

[1]. James Newsome, Elaine Shi, Dawn Song,"The Sybil Attack in Sensor Networks: Analysis & Defenses" *IPSN'04,* April 26–27, 2004, Berkeley, California, USA.

[2]. Mina Rahbari1 and Mohammad Ali JabreilJamali," Efficient Detection Of Sybil Attack Based On Cryptography In Vanet" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011

[3]. Ali Akbar Pouyan, MahdiyehAlimohammadi,"Sybil Attack Detection In Vehicular Networks" Computer Science And Information Technology 2(4): 197-202, 2014

[4]. RoopaliGarg, Himika Sharma," Comparison between Sybil Attack Detection Techniques: Lightweight and Robust" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 3, Issue 2, February 2014

[5]. D. R. Bild, Y. Liu, R. P. Dick, Z. M. Mao, and D. S. Wallach, "The Mason test: A defense against Sybil attacks in wireless networks without trusted authorities," IEEE Trans. Mobile Computing, under review, Mar 2014

[6]. Soyoung Park; Aslam, B.; Turgut, D.; Zou, C.C., "Defense against Sybil attack in vehicular ad hoc network based on roadside unit support," Military Communications Conference, 2009. MILCOM 2009. IEEE , vol., no., pp.1,7, 18-21 Oct. 2009

[7]. HimadriNathSaha , Dr. Debika Bhattacharyya , Dr. P. K.Banerjee," Semi-Centralized Multi-Authenticated RSSI Based Solution to Sybil Attack" International Journal of Computer Science & Emerging Technologies, Volume 1, Issue 4, December 2010.

[8]. Piro, C.; Shields, C.; Levine, B.N., "Detecting the Sybil Attack in Mobile Ad hoc Networks," Securecomm and Workshops, 2006 , vol., no., pp.1,11, Aug. 28 2006

[9]. K. Kayalvizhi, N. Senthilkumar, G. Arulkumaran," Detecting Sybil Attack by Using Received Signal Strength in Manets" International Journal of Innovative Research in Science & Engineering, March 14

[10]. Sohail Abbas, MadjidMerabti, David Llewellyn-Jones, and KashifKifayat,"Lightweight Sybil Attack Detection in MANETs" IEEE Systems Journal, Vol. 7, No. 2, June 2013

[11]. Manjunatha T. N1, Sushma M. D2, Shivakumar K. M," Security Concepts and Sybil Attack Detection in Wireless Sensor Networks" IJETTCS, Volume 2, Issue 2, March – April 2013

[12]. ByungKwan Lee, EunHeeJeong and Ina Jung, " A DTSA (Detection Technique against a Sybil Attack) Protocol using SKC (Session Key based Certificate) on VANET" International Journal of Security and Its Applications Vol. 7, No. 3, May, 2013

[13]. Mukul Saini, Kaushal Kumar and Kumar VaibhavBhatnagar," Efficient and Feasible Methods to Detect Sybil Attack in VANET" International Journal of Engineering Research and Technology, Volume 6, Number 4 (2013)

[14]. Navneet, Rakesh Gill," Sybil Attack Detection and Prevention Using AODV in VANET" IJCSMS International Journal of Computer Science & Management Studies, Vol. 13, Issue 07, September 2013

[15]. S. Park, B. Aslam, D. Turgut, and C. Zou. Defense against Sybil Attack in the Initial Deployment Stage of Vehicular Ad hoc Network based on Roadside Unit Support. *Security and Communication Networks*, 6(4):523–538, Wiley, April 2013.

[16]. KaramjeetKaur , Sanjay Batish& Arvind Kakaria," Survey of Various Approaches To Countermeasure Sybil Attack" International Journal of Computer Science and Informatics, Vol-1, Iss-4, 2012