Localization System Based on User's Similar Trajectories Measurement over Road Network Model

Riaz Ahmed Shaikh, Imran Memon, Qasim Ali Arain, Deedar Ali Jamro, Hina Memon

***Abstract*—The transportation engineering and automotive companies is currently designing the intelligent vehicles that are safer, secure and efficient for daily life .The future vehicles achieve the goal to information and communication technology and intelligent transportation system. The localization system is a solution that can be used to accurately locate trajectories measurement over road network and explosions in real time. The principle of vehicular ad hoc network, which locates the user trajectories privacy over road network applications or more predefined points, is used here. The system implementation based on mathematical model user trajectories privacy modules placed around the area to be monitored, connected via a road network to a master module. The entire system is implemented as stand-alone, cost effective embedded solution, without the usage of expensive personal or industrial computers. We are given analysis various attacks and their valuable solutions.**

***Keywords*— Trajectory, location based service, similar velocity, data encryption, anonymous communication, privacy preserving**

I. INTRODUCTION

Vehicle detection and tracking has become an urban traffic control difficulties in haze scene. Vehicle tracking is always a popular subject in the field of computer vision applied in urban surveillance and monitoring, traffic control and military etc.

Manuscript Received September 06, 2016; accepted 12th October, 2016; date of current version December 2016

Riaz Ahmed Shaikh is with Department of Computer Science, Shah Abdul Latif University, Khairpur ,Pakistan (email: riaz.shaikh@salu.edu.pk)

Imran Memon is with College of Computer Science, Zhejiang University, Hangzhou, China ((email: imranmemon52@zju.edu.cn)

Qasim Ali Arain is with Department of Software Engineering, Pakistan ((email: qasim_ali_arain@yahoo.com)

Deedar Ali Jamro is with Mehran University of Engineering & Technology, Jamshoro, Pakistan (email: deedar.jamro@salu.edu.pk)

Hina Memon is with Shah Abdul Latif University, Khairpur, Institute of Mathematics and Computer Science, University of Sindh, Jamshoro, Pakistan (email: 2364420763@qq.com)

The Localization System is a solution that can be used to accurately pinpoint the source locations of user trajectories, low to medium frequency, explosions and even serious vehicular accidents and relay the location to the user in real time. It works on the principle of vehicular by which, the time Difference of arrival (TDOA) of the sound wave at three or more predefined points is used to determine the location of the sound source.

The aim of the project is to create a working solution which can be easily scaled up to monitor large areas for both civilian and military purposes. The minimum time control, impact time control and impact angle control [1-5]. In the real world it is used and its design is deployed. For example, asking more bandwidth than volunteers want to give so that it should not be costly to run, by giving permission to attackers to join the onion routers (TOR) in illegal events. Moreover, it should not put a burden on operators, for core patches, or different proxies for each protocol nor should it be problematic or expensive to implement. Transmitted data between vehicles can be intercepted by unauthorized users. Therefore, security in real time applications based road networks is a considerable factor to achieve security requirements in terms of confidentiality, authentication, availability and non-repudiation [6-8]. With the expanded utilization of the Internet for basic applications, security improvements were required for IP. To this end, an arrangement of conventions called IP Security or IPSec was produced.

The rapid development of vehicular technologies may apply modern information and interconnection to improve the safety via vehicle to infrastructure (V2I) and vehicle to vehicle (V2V) communications [8]. Vehicular network are known as Vehicular Ad-Hoc Networks (VANETs), which are mostly used in intelligent Transportation Systems (ITS) applications. In vehicular networks, the vehicles communicate with each other such as Inter-Vehicle Communication (IVC) and also with roadside base stations through road side unit .The vehicular networks provide safety for the users on the roads by providing timely information to the drivers. Vehicular network is a sub-class of mobile ad hoc networks (MANETs) and work on the same principle of mobile ad

 ISSN-2409-6520

hoc networks (MANETs).In the early stage of 2000, MANET were one to one application but now a days VANETs have grown up in terms of inter-vehicle communication. VANET supports wide range of applications such as multi-hop message broadcasting over long distance and many other technologies that might uses UMTS, LTE, or WiMAX IEEE 802.16. For short range communication, it may use WLAN (either standard Wi-Fi), Bluetooth, Visible Light Communication and Infrared. Routing protocols in VANETs are significantly different from road networks, because various applications in VANET may have different QOS requirements for safe application. Broadcast routing in VANET is unlike from routing in road network due to various reasons such as rapidly changing network topology, wide range communication, and traffic pattern in different time and places. This may imply that conventional routing protocols for road network are not appropriate for most vehicular broadcast applications and they may also have different application requirements as compared to road network such as Infotainment applications, assistance co-operative awareness and Traffic efficiency management.

All the beacon messages have common requirements which are periodic broadcast and low latency. The beacon messages are useful for safety applications, such as collision avoidance, driver assistance, and cruise control, etc. These applications require accurate and timely information, and the typical beacon broadcast frequency is in the range of 5-10 Hz [9-10]. Beacon messages are transmitted as using one-hop broadcast due to the potential beneficial to all vehicles within the transmission radius. These event-driven warning messages, called event messages, are sent when a hazardous situation is detected. The National Highway Traffic Safety Administration (NHTSA) has identified and set down requirements for Intelligent Vehicle Safety Applications, such as Approaching Emergency Vehicle Warnings, SOS Services, Electronic Emergency Brake Lights (EEBLs), and Post-Crash Notifications (PCNs). In addition, the word on a regulatory proposal that would require V2V devices in new vehicles in a future year has begun. However, if these event messages are abused by the attacker, it may raise new safety risks for the whole transportation system [11].

Trust management is one of the methods to detect an internal mischievous transport from conveying the mischievous message. Though, the existing trust management system still encounters some challenges. a) On location privacy enhanced schemes, the existing trust management systems encounter false negative and high false positive rates in discovering mischievous vehicles and determining which message is trustworthy. There is a quandary among ensuring care and protecting the privacy of drivers in VANETs. b) In a multi-hop event scenario, if adversaries forward contradict opinions faster than the trustworthy vehicles can, the honest vehicle may be misled. The same trick used to sup-port bogus event message can still work. c) On collusion attacks, if malicious vehicles collude to cheat the message receiver by altering the opinion of the event message, a vehicle will be misled due to too many malicious vehicles forwarding the event message to support the bogus messages or against the normal messages [12].

In VANETs each message need not to be verified and sent to the main server while on the other hand, in road networks every message must have to pass from main server and road side unit. These periodically broadcast messages are known as beacon messages. The content of beacon messages may include a vehicle's current position, velocity, and headway route. All the beacon messages have common requirements which are periodic broadcast and low latency. The beacon messages are useful for safety applications, such as collision avoidance, driver assistance, and cruise control, etc. These applications require accurate and timely information, and the typical beacon broadcast frequency, that might be in the range of 5-10 Hz [13]. The National Highway Trace Safety Administration (NHTSA) has identified and set down requirements for Intelligent Vehicle Safety Applications [14].In addition, the work on a regulatory proposal that would require V2V devices in new vehicles in a future has already been started.

In Mix-zone server, two classical address configuration protocols such as state full protocol and other is stateless protocol established on duplicate address detection [14]. To consider latency and high cost, such protocols could not efficiently work in multi-hops network and road network environment. To reduce the cost and delay and to achieve address configuration in the road networks is an important challenge. Various messages for road conditions, congestion avoidance and detour notification for road authorization can spread by VANETs [15]. The value added services and traffic associated message delivered by road network are used to improve drivers wayfaring capability, toll payment services and provide internet access navigation etc. To address above challenges, this manuscript has proposed an effective protocol and anonymous authentication scheme for road network. Our scheme has significant feature that may compared with existing methods; (i) An anonymous authentication, it provides content secrecy communication (ii) It accomplishes low storage requirements.

The IPSec technology is the one that brings secure communication to the internet protocol. The arrangement was intended to be usable for both IPv4 and IPv6. The IPSec is not a solitary convention, yet rather an arrangement of administrations and conventions that give an entire security answer for an IP organize. However, road networks are still limited in terms of energy and memory storage capability [15]. In order to establish an efficient security scheme based WSNs, it is necessary to understand carefully the process of security functions in terms of time execution, and uploaded program size[16-17].|In addition, there is no need for non-anonymous parties (just like websites) for our software to be run. This goal cannot be achieved for known users talking to unidentified servers; however, due to meeting point design [18].

 ISSN-2409-6520

II. RELATED WORK

a. Road network

In order to actively validate a received message, opinion piggybacking re-quires that each entity forwarding a message appends its own opinion to the message and decides whether or not to trust the message based on the attached opinions.

Contemporary location based systems (LBS) are named as versatile area administrations, remote area administrations and area mindful applications. They may likewise be named as programming applications, area mindful advances, versatile correspondence frameworks and handheld cell phones [18]. Area based frameworks are additionally utilized by a satellite situating innovation which finds the position of protest and individuals, for example, Global Positioning System (GPS) and Geographical Information System (GIS) which involves databases loaded with physical area information. In LBS is for the most part characterized as an application, which gives the data administrations identified with and dependent upon the area of the substance or area data worried with the explorer. In this unique circumstance, the creator has overlooked indoor innovations like Bluetooth, RFID and Wi-Fi and limits the exploration to open air area based frameworks where data with respect to situating can be measured by the portable system or some other gadget to decide the area of cell phone. From now on, to guarantee the protection of area, nom de plumes made in an officially characterized way [19-21]It handicaps trespasser to interface with the present pen name a vehicle and the once in the past created pen name by a similar vehicle. In actuality, the adjustment in pen names not creates the vigorous arrangement on the grounds that frequently, the vehicles may have unique directions and speed. In this manner, an attacker can compute the position utilizing physical relationship. Keeping in mind the end goal to evade such obstructions, another system is proposed in [22], where the vehicles stays quiet for particular time inside blend zones after which it will change nom de plume close time by utilizing least K-1 different clients .This idea gave specialists another bearing towards settled blend zone idea which despite what might be expected, is limited to be actualized just at way intersections [23].

Settled blend zones depict certain general components including zones which are connected at pre-chosen positions, and the activity that enters the framework must change their aliases crossing points are considered for blend zones). Additionally, vehicles inside the settled blend zone need to stay noiseless and all correspondence applications stay latent or disengaged. An essential clash that emerges here is that when the pen name a vehicle terminates before it goes in with the general mish-mash zone, the vehicle may transmit the security message utilizing its past nom de plumes it will change to the new aliases. To keep away from such uncertainty, the idea of cryptographic settled blend zones is actualized at convergences of streets [24].By actualizing the idea of cryptographic settled blend zones, message would get encoded. In this way, the vehicles inside this zone can transmit security data which is in opposition to the possibility of the settled blend zones. It makes the idea of cryptographic settled blend zone unfeasible. Along these lines, another critical expansion was made by a scholar, who recommended an accumulation vehicles can be driven by a head-vehicle, giving the chance to alternate autos to remain calm for a long stretch of interim[25]. It was watched that this thought neglected to accomplish craved yield in time touchy security applications, bringing about top of the line to-end delay. Aside from that, if head-vehicle is caught by some assailant, then the security and protection of every single other vehicle inside that gathering will likewise be at stack.

Scanning for comparable directions of moving items is firmly associated with two research issues:

1. Speaking to the direction of movable articles
2. Characterizing estimations of likeness

Regarding the primary issue of research, numerous reviews have examined approaches that the directions of movable items can be spoken to [26]. Specifically, illustration models for directions has been proposed in view of Markovian and non-Markovian likelihood models in [27]that can be viable in removing helpful data from directions. Additional model of fascinating has been discussed in that reflects the life savers of geospatial of different granularities. These strategies manage moving items on the Euclidean distance. In any case, majority of moving items in genuine transport applications, for example, trains or vehicles, are located in street arrange space as opposed to in the Euclidean distance. This has few examinations in regards to speaking to and taking care of the development of articles in street arranges space [28]. A approach for speaking to and questioning moving articles on street systems is obviously introduced in [29]. The illustration of articles which are movable along a street system was additionally exhibited in [30]. A closest neighbor scan technique for moving articles on street systems was presented in (. With respect to another research problem, the most vital investigations of look techniques for comparable directions are originated in [31]. A strategy for discovery the maximum comparable direction of a given inquiry direction inside a repository utilizing the longest normal subsequence approach has been proposed in [31]. Be that as it may, this strategy has two issues when used to scan for comparative directions of moving articles on street systems. To begin with, this technique does not take worldly or spatiotemporal factors into thought. For instance, two directions going through a similar range at various circumstances are viewed as comparable. Second, since this technique depends on Euclidean space, it can't be utilized to scan for comparable directions on street organizes as talked about in the past segment.

A technique for measuring the comparability between directions in light of shape was characterized in [32]. The upside of this definition is that spatiotemporal viewpoints are considered, dissimilar to [33]. In any case, since this strategy accept Euclidean space, it is hard to apply it to street organize space. A comparable technique was proposed in yet has an indistinguishable issue of Euclidean separation from [34].

 ISSN-2409-6520

b. Similarity of Moving Object Trajectory on Road Networks

Most moving items are in street organize space as opposed to in Euclidean space. There are a few contrasts between Euclidean space and street organizes space. In the first place, figure 1 delineates the diverse meanings of separation in Euclidean and street organize space. In figure 1, the genuine separation from a to b is not 4 km but rather 9 km. Second, unique organize frameworks are utilized for street arrange space. While the (x, y, t) organize framework is the most prominent one in Euclidean space, (Sid, d, t) is more productive in street arrange space, where Sid is a street segment identifier, and d is the counterbalanced from the beginning stage of the street part. Inquiries are given by indicating the street part ID instead of a range in Euclidean space. It is simpler to ascertain separate between two focuses on street arranges by utilizing street organize facilitate frameworks than Euclidean facilitate frameworks. At last, street arranges space requires extra information to portray the availability between street areas. These differences should be carefully examined and considered when analyzing trajectories in road network space [35-36].

c. Vehicular network

Therefore, another idea of client driven approach named as swing and swap was advanced which has opened up the mystery by permitting vehicles to daintily organize their redesigns by changing their speed. In any case, adjustment in vehicle's speed like that of its way is not satisfactory. The time span required for broadcasting a security message comprises of a couple of microseconds, being too short to be viewed as a noiseless period. Along these lines, the technique portrayed in falls flat not just on the grounds that the pen names vehicles remain calm for a little time additionally in light of the fact that this approach is illogical when cars are on parkway or on a solitary street. The fundamental thought proposed by the creator is transport v and its neighbors need to change their nom de plumes until there must be at littlest K-1(1>=K) vehicles [37-38]. Henceforth, in the above characterized situation, when vehicles v's neighbors are in little number, for example, on account of a low activity street, this approach gets to be distinctly unfeasible to apply or gives deficient security level if executed. A more vigorous idea in view of element blend zone is given in [39] to stay away from this impediment. For this situation, each substance can evaluate its characterized blend zone by utilizing a trusted middle person. In the above characterized situation, it is not obligatory for each vehicle to remain quieted in the mixzone in this way that could be actualized for a promising yield. Yet, this approach has likewise its confinements because of the way that, a narcissistic vehicle may not collaborate amid pen name due to vast overhead happening during the time spent alias[40].

A great deal of work has been done, which concentrates on conceited and narrow minded vehicles in the blend zone [41]. In any case, actually, these strategies for securing secrecy are far excessively costly and troublesome. To address such issues, another method has been proposed in. On the premise of amusement hypothesis, the creator dissected the area of blended zones in the ideal districts and has likewise expected the event of neighborhood enemy. He additionally had foreseen a decision about the ideal conduct of the vehicles and the assailant. Additionally construct his review in light of diversion hypothesis inducing that vehicles utilize pen names of the attributes of social spots. In any case, both methodologies neglected to consider vehicle's changing area security. In this way, building blend zone for vehicles by utilizing cryptographic approach has been proposed in. It is additionally, proposed to build cryptographic blend zones by putting distinctive street side units (RSU) at the focuses where uncommon movement thickness is watched. Once cryptographic blend zone has been drawn nearer by the vehicle, RSU would dole out a symmetric key to the vehicle. For whatever length of time that the vehicle stays inside this blend zone, whole correspondence remains scrambled and a foe may not adjust information in the message. Vehicles inside the blend zone will speak with the vehicles outside the blend zone being in direct range and may decode the messages. Subsequently, the messages may likewise be traded and unscrambled by the vehicles. In the meantime, vehicles will change pen names remaining inside the blend zone. A further research around there prompted to a foundation less approach which has been introduced against the worldwide enemies in [42]. In this approach, vehicles are assembled together for a brief timeframe alongside keeping up the noiseless period. In this situation, every one of the vehicles stays noiseless with the exception of the gathering pioneer which communicates data. Also, the rest of the vehicles will present the time of quiet, uncovering less data for the enemy, when vehicles change their nom deplumes.

While utilizing aliases, can separate the area information from a specific client. In the possibility of powerfully changing nom de plumes a blended zone was at first presented, where various clients meet, limiting a foe from associating numerous aliases a similar client. Be that as it may, this thought is just pertinent when opponent has only a restricted perspective of client's development and breaks down nom de plumes vehicles while entering and leaving a similar blend zone [43-50]. In creators have proposed the way disturbing system that adds certain clamors to real area information so that each client can outline diverse conceivable way by swapping their nom de plumes they meet at a similar place. This system, in any case, may not consider a rival's outside data that can interface every client with a specific area. In the idea comprises of area anonymization and is being utilized by a few different analysts. As of late, research has been directed on area namelessness that spotlights on street systems [51-52]. The idea of Xstar has been offered in which proposed hiding the areas in view of QoS necessities and streets arrange security. It keeps up the dependability among the handling expense of unidentified question and the assault versatility of the performed wellbeing [53-54].

 ISSN-2409-6520

III. USER'S SIMILAR TRAJECTORIES MEASUREMENT MODEL

In this paper, User Similar Trajectories UST(x) is the class of all interval road sets of universal *X*, *F(X)* is the class of all road Sets of universal *X;* and in this section we will review the definition of UST and some traditional measures.

Definition 2.1.The road sets A in UST(X) is defined as [27, 43, 44]

$$A=\{\langle x, «_A(x), ¬_A(x)\rangle \mid x\in X\} A_C=\{\langle x, ¬_A(x), «_A(x)\rangle \mid x\in X\}$$

Where $«_A(x): X \to [0,1] and v_A(x): X \to [0,1]$ define the degree of membership and the non-membership of $x \in X$, and for all $x \in X$, $0 \le «_A(x)+¬_A(x) \le 1$ obviously, each road set A in *F (X)* may be represented as the following road set: $A=\{\langle x, «_A(x), 1-v_A(x)\rangle \mid x \in X\}$

Then, we will inform some basic terms:

$A \subseteq B$ If and only if $«_A(x) \le «_B(x) and ¬_A(x) \ge ¬_B(x)$ for all $x \in X$ $A=B$ if and only if $«_A(x)=«_B(x)$ and $¬_A(x) \ge ¬_B(x)$ for all $x \in X$ $A_C=\{\langle x, v_A(x), «_A(x)\rangle \mid x \in X\}$

In this paper, we then will show some traditional measures for UST(X).

Definition 2.2

Now, a function *S (A.B)* is going to represent $\mathrm{UST}(X)\times \mathrm{UST}(X) \to [0,1]$, if *S* satisfied these following requires, and then *S* is a way to measure similarities of two USTs.

S (A, A$_C$) =0 if A is a crisp sets

S (A, B) =1 if and only if $A=B$

S (A, B) = S (B, A)

For all $A,B,C \in \mathrm{UST}(X)$, if $A \subseteq B \subseteq C$, then $S(A,C) \le S(A,B), S(A,C) \le S(B,C)$ next, we will give some previous measure for UST: Let $X=\{X1,..,Xn\}$ be a discrete set of universe. Consider two vehicles A and B in UST(X).

1. Dengfeng, and Chuntian proposed, a similarity measure between A and B as follows:

$$S_d^p(\tilde{A},\tilde{B})=1-\frac{1}{\sqrt[p]{n}}\sqrt[p]{\sum_{i=1}^{n}|m_{\tilde{A}}(i)-m_{\tilde{B}}(i)|^P},$$

Where

$m_{\tilde{A}}(i)=(«_{\tilde{A}}(x_i)+1-v_{\tilde{A}}(x_i))/2, m_{\tilde{B}}(i)=(«_{\tilde{B}}(x_i)+1-v_{\tilde{B}}(x_i))/2$ and $1 \le p<\infty$

2. Liang and Shi proposed a similarity measure between A and B as follows:

$$S_e^p(\tilde{A},\tilde{B})=1-\frac{1}{\sqrt[p]{n}}\sqrt[p]{\sum_{i=1}^{n}(¤_{\tilde{tAB}}(i)+¤_{\tilde{fAB}}(i))^p}$$

Where

$¤_{\tilde{tAB}}(i)=|«_{\tilde{A}}(x_i)-1«_{\tilde{B}}(x_i)|/2$ and $¤_{\tilde{fAB}}(i)=|(1-v_{\tilde{A}}(x_i))-(1-v_{\tilde{B}}(x_i))|/2$

There are also some other previous ways which is similar to the way one and two and more simple.

3. $\sum \frac{uA(X)\wedge uB(X)+vA(x)\wedge vB(x)}{uA(X)\vee uB(X)+vA(x)\vee vB(x)}$

4. $S_A=\sum(1-\frac{|(«_A(x)-«_B(x))-(v_A(x)-v_B(x))|}{2})$

And Recently, Hung and Yang proposed two exponential-type similarity measures between UST, the first one is (5)

$$S_{hyt}(\tilde{A},\tilde{B})=1-\frac{1-\exp\left(-\sum_{i=1}(|«_{\tilde{A}}(x_i)-«_{\tilde{B}}(x_i)|+|v_{\tilde{A}}(x_i)-v_{\tilde{B}}(x_i)|/2\right)}{1-\exp(-n)}$$

And the second one is (6)

We assure that these measures satisfied these basic requirements in the definition. However these several solution is not so good for some reason and we will discuss about the drawbacks later in the example section.

IV. A NEW SIMILARITY MEASURES FOR USER TRAJECTORIES

a. Definition of our new measure

We still use Definition2.1 as the definition of UST in this section. Now, when we consider what it takes to determine similarity of two USTs, we can find their membership and non-membership can definitely determine their similarity. When we take a step further, we can find that their membership and non-membership can determine the center of membership degree of an element x∈X, and how big is the uncertainty of the membership.

So now, there are two steps for my measure. Let's assume there are two USTs:

$$A=\{\langle x, «_A(x), v_A(x)\rangle \mid x \in X\}$$

$$B=\{\langle x, «_B(x), v_B(x)\rangle \mid x \in X\}$$

For each element x :

Find out which membership interval is longer. The length of a membership of A is

$L_A=1-«_A(x)-¬_A(x)$, the same way for L_B now just consider $L_A \le L_B$, we now take the step 2

$$S(A,B)=\sum 1-\frac{\int_{«_B}^{(1-¬_B-¬_A)}|\frac{«_A+1-¬_A}{2}-\frac{2x+L_A}{2}|\,dx}{L_B-L_A}$$

If $L_B \le L_A$, we just consider B as previous A and A as previous B.

b. Therorem.1

Our new approach is also a way to measure the similarity of two USTs.

ISSN-2409-6520

Proof:

1. $S(A, A_C) = 0$ If A is a crisp set $S(1,0,0,1) = 1-1 = 0$

2. $S(A,B) = S(B,A)$ Since in our measure, we first find out which membership is looser, so obviously $S(A,B) = S(B,A)$

3. $S(A,B) = 1 \text{ if } A = B$

If $A = B$ then $S(A,B) = \sum(1 - |\frac{\alpha_A + 1 - \neg_A}{2} - \frac{2x + L_A}{2}|)$

And now $x = \alpha_B = \alpha_A$, so that $S(A,B) = 1$;

4. for all $A, B, C \in \text{UST}(X), \text{if } A \subseteq B \subseteq C,$ then $S(A,C) \le S(A,B), S(A,C) \le S(B,C)$

According to the definition $A \subseteq B$ if and only if $\alpha_A(x) \le \alpha_B(x) and \neg_A(x) \ge \neg_B(x)$ for all $x \in X$, now we just assume $L_A \le L_B \le L_C$. In fact, this function has its own actual meaning and it is not as complex as it might be seen. We assume the center of the membership of $x \in A$ is changeless if $L_A \le L_B$ and the center of A is $\frac{\alpha_A + 1 - v_A}{2}$ and we assume the center of membership of $x \in B$ is changeable since $x \in B$ has a looser membership, so the center of $x \in B$ is $\frac{2x + L_A}{2}$

Here x is from α_B to $\alpha_B + L_A$ which state the unclear of the longer one.

If we calculate the distance of center of A and B, then we must add all the condition of x then calculate the average of center and this is how this function come. Now, once $A \subseteq B \subseteq C$, it is not hard to find that the average distance of center of *A* and *C* will definitely bigger than *A* and *B*, so $S(A,B) \ge S(A,C)$, and as the same $S(B,C) \ge S(A,C)$. Only when $\alpha_A(x) \in [1,1] and \alpha_B(x) \in [0,0]$ or $\alpha_A(x) \in [1,1] and \alpha_A(x) \in [0,0]$ then. *S (A, B) = 0*

Proof: at first, we have proved

When $\alpha_A(x) \in [1,1] and \alpha_B(x) \in [0,0]$ or $\alpha_B(x) \in [1,1] and \alpha_A(x) \in [0,0]$ then *S (A, B) = 0*. Now as we have discussed from last section, this function is to calculate the average distance of two USTs only when $\alpha_A(x) \in [1,1] and \alpha_B(x) \in [0,0]$, we can find their distance is 1, in any other situation, the distance is definitely smaller than 1 which means the distance is from 0 to 1.

c. cases

In this section we will come up with some UST using the procedure we describe above and after we calculate the entire example, we will explain why our measure is better than the previous measures. For convenience and a better comparison effect, we use examples from previous articles and we are going to consider all UST have three elements and p=1, I =1, 2, 3.

Case.1

$A_1 = \{(x_1, 0.3, 0.3), (x_2, 0.2, 0.2), (x_3, 0.1, 0.1)\}$

$A_2 = \{(x_1, 0.2, 0.2), (x_2, 0.2, 0.2), (x_3, 0.2, 0.2)\}$

$A_3 = \{(x_1, 0.4, 0.4), (x_2, 0.4, 0.4), (x_3, 0.4, 0.4)\}$

$B = \{(x_1, 0.3, 0.3), (x_2, 0.2, 0.2), (x_3, 0.1, 0.1)\}$

According to the measure ways we have given early we can get the result:

$S_{pd}(A_1, B) = S_{pd}(A_2, B) = S_{pd}(A_3, B) = 1$

$S_{pe}(A_1, B) = 1$

$S_{pe}(A_2, B) = 0.933$

$S_{pe}(A_3, B) = 0.800$

$S_3(A_1, B) = 1$

$S_3(A_2, B) = 0.722$

$S_3(A_3, B) = 0.5$

$S_4(A_1, B) = S_4(A_2, B) = S_4(A_3, B) = 1$

And our new measure's result is:

$S_{new}(A_1 \quad B) = 1$

$S_{new}(A_2 \quad B) = 0.967$

$S_{new}(A_3 \quad B) = 0.900$

From the result above, it is obvious that three UST are slightly different from each other and A_1 is more ambiguous than A_3 since the hesitation of A_1 is larger. However the measure S_{pd} and S_4 cannot distinguish the differences so this measure has its own disadvantages.

Case.2:

$A_1 = \{(x_1, 0.2, 0.2), (x_2, 0.2, 0.2), (x_3, 0.2, 0.2)\}$

$A_2 = \{(x_1, 0.4, 0.4), (x_2, 0.4, 0.4), (x_3, 0.4, 0.4)\}$

$B = \{(x_1, 0.3, 0.3), (x_2, 0.3, 0.3), (x_3, 0.1, 0.3)\}$

$S_{pe}(A_1, B) = 0.900$

$S_{pe}(A_2, B) = 0.867$

$S_3(A_1, B) = 0.644$

$S_3(A_2, B) = 0.666$

$S_4(A_1, B) = S_4(A_2, B) = 0.966$

$S_{new}(A_1 \quad B) = 0.933$

$S_{new}(A_2 \quad B) = 0.925$

In this example, we can notice that S_4 cannot distinguish the two USTs. According to the element x_3, the membership degree of x_3 of A_1 is near than the membership degree of x_3 of A_1 which means $S_1 \ge S_2$ is more sensitive. At least these two USTs should not have the same similarity with *B*. The result of S_3 is a bit too small so we are also skeptical about this way.

Case.3:

$A_1 = \{(x_1, 0.1, 0.1), (x_2, 0.5, 0.1), (x_3, 0.1, 0.9)\}$

$A_2 = \{(x_1, 0.5, 0.5), (x_2, 0.7, 0.3), (x_3, 0.0, 0.8)\}$

$A_3 = \{(x_1, 0.4, 0.4), (x_2, 0.4, 0.4), (x_3, 0.4, 0.4)\}$

$B = \{(x_1, 0.3, 0.3), (x_2, 0.2, 0.2), (x_3, 0.1, 0.1)\}$

ISSN-2409-6520

$S_{pe}(A_1, B) = 0.833$
$S_{pe}(A_2, B) = 0.933$
$S_{pe}(A_3, B) = 0.600$

$S_3(A_1, B) = 0.600$
$S_3(A_2, B) = 0.866$
$S_3(A_3, B) = 0.364$

And our new method is:
$S_3(A_1, B) = 0.600$
$S_3(A_2, B) = 0.866$
$S_3(A_3, B) = 0.364$

$S_{new}(A_1 \quad B) = 0.917$
$S_{new}(A_2 \quad B) = 0.967$
$S_{new}(A_3 \quad B) = 0.600$

In this example, the results of S_3 still get far from other results. So this way is not so appropriate for these examples.

Case.4:
$A_1 = \{(x_1,0.1,0.4),(x_2,0.4,0.3),(x_3,0.3,0.1)\}$
$A_2 = \{(x_1,0.3,0.4),(x_2,0.3,0.4),(x_3,0.1,0.1)\}$
$B = \{(x_1,0.2,0.2),(x_2,0.2,0.2),(x_3,0.2,0.2)\}$

$S_{pe}(A_1, B) = S_{pe}(A_2, B) = 0.867$
$S_3(A_1, B) = 0.590$
$S_3(A_2, B) = 0.547$

Our new way's result is:
$S_{new}(A_1 \quad B) = 0.933$
$S_{new}(A_2 \quad B) = 0.925$

The two USTs compared with B is not the same and their membership and non-membership degrees have some differences, so we cannot say the two USTs should have the same similarity with B So S_{hy1} and S_{hy2} cannot work well in this example and at last as for S_3. Although we cannot directly say it is wrong, we can notice that in several examples, the result of that way is totally far from any other ways and the result is not match our general thinking, so S_3 also has its own disadvantage.

So from all of the examples above, our new method can match all the examples require and other traditional methods have its own disadvantage.

c. Trust Attacks

It is nothing that the trust attacks may incorporate with various attacks by attackers, such as dropping benign event message by ADoS and incorporate with message alteration attacks (Aalt). Due to wireless band-width jamming attacks make all the wireless network transmission unavailable, which might beyond the extent of this research work and has been omitted.

d. Evaluation on Detection Accuracy

At the point when a vehicle gets an occasion message, the framework processes the trust-value of the got occasion message and chooses whether the message is reliable or not. On the off chance that the basic leadership vehicle chooses the occasion message is reliable; it advances the occasion message with a positive supposition to bolster the occasion, else it will be perceived as a malignant occasion message and forward the occasion message with their inverse feeling keeping in mind the end goal to caution the neighboring vehicle. Amid the recreation, both typical and assault messages are transmitted in the VANETs.

In this paper, keeping in mind the end goal to consider both accuracy and review rate of the reproduction comes about, we embrace F1-measure (signified as F1) [29], as appeared in Equation (11), to quantify the general execution of the proposed plot, which depends on van Rijsbergen's effectiveness measure. It is essential to assess accuracy and review together, due to the ease of upgrading it is possible that one independently.

e. Evaluation on Decision Delay

To assess the location postponement of the proposed show, we likewise assess the time delay between the rest of occasion message accepting time and the basic leadership time. In misbehavior detection systems, the window of vulnerability is the overall time consumption of all steps [17]. It is noted that both global reporting and revocation have necessarily required infrastructure support in the simulation and might be in influenced by the bandwidth limit. In this paper, in order to simplify the simulation environment, we focus on investigating the influence of decision delay. To evaluate the time efficiency, mean decision delay (MDD) is used to calculate the average delay of all the decisions.

V is the set of overall simulated vehicles; j V j is the amount of vehicles in the specific scheme. And N is the set of received event, and jNj is the amount of the event in N. tdec is the decision timestamp that decides to accept or warn for the event message, and t1st is the timestamp of the received message of the same event n. It is noted that, in this evaluation, the computational delays of the signature verification does not included in the evaluation due to the same signature verification process of each system model.

V. TYPES OF SECURITY THREATS/ATTACKS ON TOR

a. Passive Attacks

Tracking user's traffic: By monitoring user's connection show not show his/her data but will show the similar traffic patterns.

Monitoring user's data: Data at the end is encrypted, not the connection. In order to hide application data traffic, Tor can use Privacy and filtering services.

Selections distinguish ability: Tor allows clients to select configuration selection. With this clients who are

 ISSN-2409-6520

fewer might give up maximum anonymity by looking different. End-to-end timing correlation: The safety currently presented against such analysis to hide the link between the OP and the first entry node by running a Tor relay or behind the firewall. End-to-end size correlation: Observing the data packets will be useful in the analysis of end points of traffic.

b. Active Attacks

Compromise keys: An attacker who comes to know a relay's identity key replaces that relay forever.

Run a recipient: An opponent controlling a web server knows the timing outlines of the users who are linking to it, and can introduce random outlines in its replies.

Run an onion proxy: Sometimes, it might be necessary for the proxy to execute remotely. Identification of onion proxy is the identification of all the links that will occur as a consequence. Denial of service: An attacker can over load the random nodes to cut off its link from the network.

c. Index Directory Attacks

Destroy index servers: If some index servers vanished, the remaining can still convey the details of the network and create a consensus index. If most of them are destroyed, then the directory will not have enough signatures for the users. Subvert an index server: By hijacking a directory server, an opponent can influence the last index to some extent.

d. Attacks against meeting points

Make many requests: An opponent can cut off the Bob service by overloading his entry points with requests. Compromise a meeting point: A meeting point is not going to respond further on a circuit, since all data traffic is encrypted going through the meeting point with a session key which is a mutual key of Alice and Bob.

VI. CONCLUSION

In this paper we develop localization system is a solution that can be used to accurately locate trajectories measurement over road network and explosions in real time. The principle of vehicular ad hoc network, which locates the user trajectories privacy over road network applications or more predefined points, is used here. The system implementation based on mathematical model user trajectories privacy modules placed around the area to be monitored, connected via a road network to a master module. In the future, we will adopt this approach to cluster similar trajectories and find the representative trajectory to infer future locations of moving objects and their privacy level.

ACKNOWLEDGMENT

We are finally thankful to the editor, reviewers and IBT especially who provided us with the opportunity to publish our research paper in this esteemed journal.

REFERENCES

[1] Y. Liu, Y. Li, H. Man, June, 2005, "Mac layer anomaly detection in ad hoc networks, in: Proceedings of the 6th Annual IEEE SMC Information Assurance Workshop (IAW '05)", West Point, NY, USA, 15–17, pp.402–409.

[2] Zhenjun Han, Jianbin Jiao, Baochang Zhang, et al, 2011," Visual object tracking via sample-based Adaptive Sparse Representation (AdaSR)". Pattern Recognition, Vol. 44(9), pp. 2170-2183.

[3] M.S. Arulampalam, S. Maskell, N. Gordon, and T. Clapp,2002, "A tutorial on particle filters for on-line non-linear/non-Gaussian Bayesian tracking", IEEE Trans. Signal Process., vol.50(2), pp.174-189.

[4] Yanwen Chong, Wu Chen, Zhilin Li, et al., 2013, "Integrated real-time vision-based preceding vehicle detection in urban roads". Neurocomputing, Vol.116, pp. 144-149.

[5] Salti, S., Cavallaro, A., Stefano, L. D., 2012, "Adaptive appearance modeling for video tracking: Survey and evaluation". IEEE Transactions on Image Processing, Vol.21 (10), pp.4334–4348.

[6] Matthews, I., Ishikawa, T., Baker, S., 2004, "The template update problem". IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.26, pp.810–815.

[7] K.Nummiaro, E.Koller-Meier, and L.V.Gool, 2003, "Object tracking with an adaptive color-based particle filter", Proc. Symposium for Pattern Recognition of the DAGM, pp.591-559.

[8] Li Min, TanTieniu, Chen Wei, et al., 2012, "Efficient object tracking by incremental Self-Tuning particle filtering on the affine group". IEEE Transactions on Image Processing, Vol. 21(3), pp.1298–1313.

[9] Mei, X.,Ling,H., 2011 ," Robust visual tracking and vehicle classification via sparse representation". IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 33(11), pp.2259–2272.

[10] B.Babenko, Yang Ming-Hsuan, S.Belongie., 2011," Robust Object Tracking with Online Multiple Instance Learning". IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 33(8), pp.1619–1632.

[11] Alex X. Liu, Amir R. Khakpour, 2013."Quantifying and verifying reachability for access controlled networks" .IEEE/ACM Transactions on Networking (TON), Vol.21 (2).

[12] Myounggyu Won, Radu Stoleru, 2014."A Low-Stretch-Guaranteed and Lightweight Geographic Routing Protocol for Large-Scale Wireless Sensor Networks" .Transactions on Sensor Networks (TOSN) , Vol.11(1).

[13] Nejc Škoberne, Olaf Maennel, Iain Phillips, Randy Bush, Jan Zorz, Mojca Ciglaric, 2014, "IPv4 address sharing mechanism classification and tradeoff analysis" .IEEE/ACM Transactions on Networking (TON), Vol.22 (2)

[14] Young-Sik Jeong, Ji Soo Park and Jong Hyuk Park. 10 March 2015." An efficient authentication system of smart device using multi factors in mobile cloud service architecture",

 ISSN-2409-6520

INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS.Vol.28 (4), Pp. 659–674.

[15] Hung-Min Sun, Chiung-Hsun Chen, Chih-Wen Yeh, Yao-Hsin Chen, 2013, "A collaborative routing protocol against routing disruptions in MANETs" .Personal and Ubiquitous Computing , Vol. 17(5).

[16] Shin, H., Talipov, E.,&Cha, H, 2012, "Spectrum: Lightweight hybrid address auto configuration protocol based on virtual coordinates for 6LoWPAN". IEEE Transactions on Mobile Computing, vol.11(11), pp.1749–1761.

[17] Imran Memon, Ling Chen , Abdul Majid ,Mingqi Lv , Ibrar Hussain , Gencai Chen, 2014, "Travel Recommendation Using Geo-tagged Photos in Social Media for Tourist". Wireless Pers Commun .DOI 10.1007/s11277-014-2082-7

[18] Talipov,E., Shin, H., Han, S., et al, 2011, "Alightweight stateful address auto-configuration for6LoWPAN".Wireless Network, vol.17(1), pp.183–197.

[19] Al-Mistarihi, M. F., Al-Shurman, M., & Qudaimat, A, 2011, "Tree based dynamic address auto-configuration in mobile ad hoc networks". Computer Networks, vol.55(8),pp. 1894–1908.

[20] Mohandas, B. K., & Liscano, R, 2008, "IP address configuration in VANET using centralized DHCP". In 33rd IEEE local computer networks conference, pp. 608–613.

[21] Romain Coussement, Boucif Amar Bensaber, Ismail Biskri, 2013, "Decision support protocol for intrusion detection in VANETs" .DIVANet '13: Proceedings of the third ACM international symposium on Design and analysis of intelligent road network and applications.

[22] Jianghong Wei, Xuexian Hu and Wenfen Liu, 2014,"Two-factor authentication scheme using attribute and password" .INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS.DOI: 10.1002/dac.2915.

[23] Qi Xie, Na Dong, Duncan S. Wong and Bin Hu, 2016,"Cryptanalysis and security enhancement of a robust two-factor authentication and key agreement protocol". INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS. Vol.29 (3), pp.478–487.

[24]Abderrahmane BenMimoune, Fawaz Ali Khasawneh, Michel Kadoch, Songlin Sun, Bo Rong, 2014,"Inter-cell handoff performance improvement in LTE-a multi-hop relay networks". MobiWac '14: Proceedings of the 12th ACM international symposium on Mobility management and wireless access.

[25] Jun Han, Yue-Hsun Lin, Adrian Perrig, Fan Bai, 2014,"Short paper: MVSec: secure and easy-to-use pairing of mobile devices with vehicles" .WiSec '14: Proceedings of the 2014 ACM conference on Security and privacy in wireless & mobile networks.

[26] Imran Memon, Farman Ali Mangi, Deedar Ali Jamro, 2013,"Collision Avoidance of Intelligent Service Robot for Industrial Security System". IJCSI International Journal of Computer Science Issues, Vol. 10(2), No 3.

[27] Memon, I, 2015, "Authentication user's privacy: An integrating location privacy protection algorithmFor secure moving objects in location based services". Wireless Personal Communications, Doi: 10.1007/s11277-015-2300-y

[28] Imran Memon, Farman Ali Mange, Deedar Ali Jamro, Muhammad Abdul Basit, Muhammad Hammad Memon. June, 2013,"Rumor Riding: Peer to Peer Systems" .International Journal of Scientific & Engineering Research, Vol.4 (6).

[29] Tzonelih Hwang · Prosanta Gope, 2013, "Provably Secure Mutual Authentication and Key Exchange Scheme for Expeditious Mobile Communication Through Synchronously One-Time Secrets" .Wireless Pers Communication.vol.77,pp.197–224.DOI 10.1007/s11277-013-1501-5

[30] Xiaonan, W., & Shan, Z., 2013, "An MZs address configuration scheme for wireless sensor networks based on location information". Telecommunication Systems, vol.52 (1), pp.151–160.

[31] Ben-Jye Chang , Ying-Hsin Liang , Houng-Jer Yang, 2013, "Performance Analysis with Traffic Accident for Cooperative Active Safety Driving in VANET/ITS" .Wireless Pers Communicatioon,vol.74,pp.731–755 DOI 10.1007/s11277-013-1318-2.

[32] Bidi Ying, DimitriosMakrakis, HusseinT.Mouftah, 2013,"Privacy preserving broad cast message authentication protocol for VANETs" .Journal of Network and Computer Applications.vol.36, pp.1352–1364.

[33] Rakesh Kumar, Mayank Dave, 2013,"A Framework for Handling Local Broadcast Storm Using Probabilistic Data Aggregation in VANET".Wireless Pers Communication. Vol.72, pp.315–341 DOI 10.1007/s11277-013-1016-0

[34] Chena, Y.-S., Hsu, C.-S., Yi, W.-H, 2012, "An IP passing protocol for vehicular ad hoc networks with network fragmentation". Computers and Mathematics with Applications, vol. 63(2), pp.407–426.

[35] XiaonanWang , Yi Mu , Guangjie Han , Deguang Le, 2014, "A Secure MZs Address Configuration Protocol for Road network" .Wireless Pers Commun DOI 10.1007/s11277-014-1882-0

[36] Xiuchao Wu, Kenneth N. Brown, Cormac J. Sreenan, Pedro Alvarez, Marco Ruffini, Nicola Marchetti, David Payne, Linda Doyle, 2013, "An XG-PON module for the NS-3 network simulator".SimuTools '13: Proceedings of the 6th International ICST Conference on Simulation Tools and Techniques..

[37] Dheerendra Mishraa,Ankita Chaturvedib, Sourav Mukhopadhyayb. August, 2015,"Design of a lightweight two-factor authentication scheme with smart card revocation". Journal of Information Security and Applications Vol.23, Pp. 44–53.

[38] Nikolaos Karapanos, Claudio Marforio , Claudio Soriente , Srdjan Čapkun, August 12-14 , 2015, "Sound-proof: usable two-factor authentication based on ambient sound", Proceedings of the 24th USENIX Conference on Security Symposium,Washington, D.C, , pp.483-498.

 ISSN-2409-6520

[39] Thanasis Petsas , Giorgos Tsirantonakis , Elias Athanasopoulos , Sotiris Ioannidis, April 21-21, 2015,"Two-factor authentication: is the world ready?: quantifying 2FA adoption", Proceedings of the Eighth European Workshop on System Security, Bordeaux, France, p.1-7.

[40] Qi Jiang, Jianfeng Ma and Youliang Tian, 2015, "Cryptanalysis of smart-card-based password authenticated key agreement protocol for session initiation protocol ". INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS. Vol.28(10), Pp. 1340–1351.

[41] SHIRVANIAN, M., JARECKI, S., SAXENA, N., AND NATHAN, N, 2014, "Two-factor authentication resilient to server compromise using mix-bandwidth devices". In The Network and Distributed System Security Symposium NDSS '14.

[42] De Cristofaro, E., Du, H., Freudiger, J., and Norcie, G, 2014,"A comparative usability study of two-factor authentication". In Proceedings of the Workshop on Usable Security (USEC) .

[43] Eric Grosse , Mayank Upadhyay,2013, " Authentication at Scale", IEEE Security and Privacy, Vol.11(1), pp.15-22, [doi>10.1109/MSP..162]

[44] N.S. Khandelwal, P.Kamboj, 2015,"Two factor authentication using Visual Cryptography and Digital Envelope in Kerberos". International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO).pp.1 – 6.

[45] Chi-Tung Chen1 and Cheng-Chi Lee. 25 May 2015,"A two-factor authentication scheme with anonymity for multi-server environments". Security and Communication Networks Vol. 8(8), pp. 1608–1625,

[46] Liping Zhang, Shanyu Tang, Jing Chen, Shaohui Zhu, 2015, "Two-Factor Remote Authentication Protocol with User Anonymity Based on Elliptic Curve Cryptography". Wireless Personal Communications, Vol.81 (1), pp 53-75.

[47] Xiong Li1,, Jianwei Niu,, Junguo Liao and Wei Liang. 25May 2015, "Cryptanalysis of a dynamic identity-based remote user authentication scheme with verifiable password update". International Journal of Communication Systems Vol.28 (2), pp. 374–382.

[48] Qi Jiang, Jianfeng Ma, Guangsong Li and Xinghua Li. 25 January 2015,"Improvement of robust smart-card-based password authentication scheme". INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS Vol. 28(2), pp.383–393.

[49] Qi Jiang, Jianfeng Ma and Youliang Tian, 10 May 2015,"Cryptanalysis of smart-card-based password authenticated key agreement protocol for session initiation protocol". International Journal of Communication Systems Vol. 28(7), pp.1340–1351.

[50] Saru Kumari, and Muhammad Khurram Khan. December 2014,"Cryptanalysis and improvement of 'a robust smart-card-based remote user password authentication scheme". International Journal of Communication Systems Vol. 27(12), pp. 3939–3955.

[51] Chun-Guang Ma, Ding Wang, andSen-Dong Zhao. October 2014,"Security flaws in two improved remote user authentication schemes using smart cards". International Journal of Communication Systems Vol.27 (10), pp. 2215–2227.

[52] Jianghong Wei, Xuexian Hu, Wenfen Liu, 2015,"Two-factor authentication scheme using attribute and password, International Journal of Communication Systems, vol.28 (18), pp.20-25.

[53] Ding Wang, Ping Wang, 2014,"Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks", Ad Hoc Networks, vol.20 (1), pp.35.

[54] Jian-Jun Yuan, January, 2014,"An enhanced two-factor user authentication in wireless sensor networks". Telecommunication Systems, Vol. 55(11), pp 105-113.

 ISSN-2409-6520