I. J. Computer Network and Information Security, **2019, 7, 29-36**
Published Online July 2019 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2019.07.05

Agent Based Trust Establishment between Vehicle in Vehicular Cloud Networks

Shailaja S. Mudengudi
Electronics and Communication Engineering Department, Tontadarya College of Engineering
Gadag, 582-101, Karnataka, INDIA
E-mail: psmssm@gmail.com

Mahabaleshwar S. Kakkasageri
Electronics and Communication Engineering Department, Basaveshwar Engineering College (Autonomous)
Bagalkot - 597102, Karnataka, INDIA
E-mail: Mahabalesh_sk@yahoo.co.in

Received: 30 March 2019; Accepted: 24 April 2019; Published: 08 July 2019

***Abstract*—**In order to enhance the driving experience with increased security and privacy, a category of MANET has emerged i.e VANET. The nodes are highly mobile, uncoordinated and dynamic in nature. An progressive step in this vision is Vehicular Cloud (VC) the advancement in Intelligent Transport System (ITS).The resources are shared between the vehicle nodes to provide the services at a economical cost. In order to provide them there should be hassle free secure communication link established between the Vehicle nodes, Road side unit (RSU) and the Cloud. Trust establishment in VC between vehicle nodes enhances the security aspects in VC. In this paper we put forth an trust evaluation scheme based on Dempster Shafer theory. The trust evaluation is based on Direct trust and Indirect trust, the priority of which can be accustomed.

Index Terms—Vehicular clouds, Encryption, Trust, Software agents.

I. Introduction

With the vision of utilizing the resources to a higher extent Olariu et al. put forth the new concept of Vehicular Cloud Computing (VCC), which is merging of the VANET with the Cloud Computing. VANET (Vehicular Ad Hoc NETwork) utilizes an inexpensive WLAN to provide communication between the vehicle nodes and the Road Side Units (RSU), to provide safe and comfortable driving experience. As the density of traffic is increasing day by day VANET is playing important role. The statistics show that an considerable expense goes for the work productivity in transportation. The other important area of matter is the congestion in normal and peak hours due to which there is impact on the fuel consumption. So it seems in inevitable to provide an infrastructure like VANET. For the communication VANET uses Dedicated Short Range Communication (DSRC) or WAVE 802.11p.The bandwidth allocated by the FCC-US Federal Communication Commission ranges from 5.850- 5.925GHz, wide spectrum large enough for accomplishing VANET applications and other enhancements [1]. With such promising advantages VANET users, still seem to be reluctant in utilizing the services to utmost extent due to security and privacy issues. As the data is put on the network the user does not have any control over it. Other issues such as intruders, confidentiality, and authenticity are also the major snag for the deployment of VANET [2]. According to NIST, Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction[3]. The NIST also lists five essential characteristics which cloud computing should possess: on-demand self -service, broad network access, resource pooling, rapid elasticity and measured service. Cloud computing make pooled resources available to user at economical cost based on demand [4]. But the personal and critical data, which is shared between the cloud entities, introduces the security and privacy concerns in cloud [5]. There are array of services delivered by cloud include platform as service, infrastructure as service, storage as service etc. Mobile cloud computing (MMC) offers the vehicle users data processing anywhere and at any time via Internet. But to provide the services MMC is depended on other technologies which are expensive and time consuming. Mobiles have limited battery life, processing capability which makes the situation worse. Vehicular Cloud Computing (VCC) provides a dedicated platform for the vehicle user with desired features to serve the drivers at a lower cost with utmost utilization of resources [6]. VCC also has two fold benefits from VANET and cloud computing. The resources provided by VCC are storage, Internet, computing etc. VCC basically deals with sensors whose status are uploaded to the cloud which makes it cost effective and fast as well. The major on demand services offered by VCC include safety related services, Traffic related services, some are specific to the users

such as infotainment etc. As the connection is mostly wireless security and privacy issues should be addressed effectively. The high mobility of the vehicle nodes and communication which is short range is of concern while designing protocols or frameworks [7]. The kinds of security issues specific to VCC are listed in [8] which include tampering of data, repudiation, privacy breach, Denial of Service (DoS), Elevation of privileges assigned to the user etc. Trust acts as an interdependent aspect in providing solution for the above security issues. Other solutions include Authentication of nodes, Access control, Digital signature, location validation etc.

Establishment of trust can be accomplished in many ways such as data centric, entity centric and sometimes both[9]. A trust management scheme classifies trust in to service provider and service requesting entity perspective. Attributes for trust calculation are SLA (service level agreement), policy, security levels, recommendation, reputation etc [10]. In all the above mentioned methods decision making is a crucial aspect. Several Decision Support Systems are available such as probability theory, fuzzy logic etc. But when the data is limited and uncertainty is present in the opinion, Dempster Shafer theory happens to be the ultimate solution. We present a frame work in this paper which establishes trust between the communicating nodes using the Dempster Shafer Theory. Mobile agents and static agents coordinate for the trust establishment which is based on Direct Trust and Indirect Trust. Where Direct Trust is the experience of the node with the node to which it is communicating, where as indirect trust it is opinion of other neighboring nodes about the destination node. In both the cases uncertainty in the opinion is considered for decision making.

Organization of the rest of paper is as follows. Related works are presented in section II, Proposed agent based trust evaluation scheme is presented in section III. Section IV the simulation results are discussed. Section V concludes the work & briefs future work.

II. Related Works

Due to its dynamic and distributed network VANET can be easily attacked. A detailed study on the security issues prevailing VANETs is presented in [11]. The authors list the entities in VANETs to whom the security is of top concern. Further kinds of attacks and attacker in VANET scenario are listed. The work also explains the requirements a security framework should posses. Some of them requirements include reliability, privacy, scalable, information correlation and verification, authenticate the communicating nodes, able to record a event etc. An classification of VCC is presented in [12] is based on Vehicular Clouds scenario, Hybrid Vehicular Clouds scenario and Vehicles which are using Clouds scenario. Further security and privacy challenges in VCC are presented which are same as the stand alone VANET and cloud computing. A detailed study on the kinds of attacks, attackers and possible solutions are presented in [13].Encryption, trust establishment, ciphers, Cryptography Hashing, Time-stamping etc can be used to elevate attacks such as Sybil attack, replay attack, DoS attack, Timing attack, Location Trailing. For on line service selection trust is taken as important criteria. In [14] a unified framework is presented as solution for establishing trust based on definition of trust and trust principals. It is based on mainly three phases. The first phase identifies the list of service providers and the services, also collects the previous trust values associated with them. In the second phase trust bootstrapping is done and evaluation of trust is done using techniques such as reputation and monitoring. In the last phase trust value is upgraded or degraded based on trust-bias, risk, feedback etc.

A novel Trust evaluation scheme is presented in [15] for VANETs based on logistic trust, which uses direct trust, indirect trust and misbehaviors of the nodes. Direct trust is evaluation is based on experience of the evaluator node with the sender node. Indirect trust accounts for experience of the sender node with the neighboring nodes. A multi-criteria based trust evaluation is presented in [16] known as AHP-Analytical hierarchy process. Three steps are used to evaluate trust value of a vehicle node to prevent false critical messages. In the first step trust is calculated based on previous record of vehicle called as reputation based trust. In the second step using PerronFrobenius theorem, direct ranking of the trust is done based on both the outcome of the message accuracy and strength of messages.

In order to make decisions regarding the events occurred effectively and quickly an adaptive decision making framework is presented in [17] with the assistance of RSU. If the outcome of the trust value is above threshold the message is forwarded else it is taken as malicious. Events such as the received opinions amount or delay between the first received message by RSUs and current received message which are transmitted by RSUs.

Based on capabilities the service models for cloud computing include Software as a Service, Platform as a Service, Infrastructure as a Service. Deployment models for clouds based on ownership are Public Cloud, Private Cloud, Community Cloud, Hybrid Cloud. Security issues in cloud computing related to data are Data Access Control, Data Integrity, Data loss, Data Theft. As solution we can use service level agreement (SLA), which is legal agreement between customer and the service provider. But once the data is put on the network other measures are to be taken such as encryption and decryption of data, Image Stegnography, Pixel Key Pattern etc [18].

In [19] Bayesian inference is used to derive the direct observation trust using forward rate and indirect trust is derived using Dempster Shafer theory. A framework for identification of a location of vehicle based on trust is presented in [20]. Here trust is calculated using on DST based three conditions belief, plausibility and uncertainty. When cryptography measures fail to detect an attack, trust can be used. A DST based framework is presented in [21] which detect black hole attacks and gray-hole attack. In some networks trust is calculated based on the strength

of the signal received, packet delivery rate. Then connection is established to the highest trusted node if it is present in the same or nearby vicinity [22].

Many Decision Support Systems (DSSs) are available for assessing risk and help in making more informative decisions considering uncertainty. Many such DSSs tools include Probability theory (PT), Analytical Hierarchy Process (AHP), Fuzzy Sets Theory (FST) and the Dempster-Shafer Theory of Evidence (DST). All the above mentioned methods have their own limitations which have been explained elaborately in [23]. Incomplete information and ignorance are typical problems in decision making. But these can be effectively handled by distributed belief assessments. Instead of simple averaging we can use aggregating risk assessments for better decision making. Dempster-Shafer Theory of Evidence (DST) could give a valid solution which can handle the uncertainty very efficiently.

Software agents have the capability of easily adapting themselves to the environment. This property makes software agents to be playing predominant role in VANETs and MANETs. A cognitive agent based BDI architecture is presented in [24], which efficiently gathers and disseminate information using the push/pull method. Quality of service based trust evaluation is followed in [25] which are reliability, integrity and availability of the resources.

III. The Proposed Work

In this section, we briefly describe about software agents, network environment, proposed trust establishment and trust evaluation scheme using agents.

A. Software Agents

An entity which is capable of acting on someone's behalf to attain a objective, for which actions may be proactive or reactive, with attributes like learning, mobility, co-operation etc., is a software agent. Agents are autonomous in nature which senses the environment and acts upon it to achieve their goals. The agent environment is generally a host system, network, a user via a graphical user interface, a collection of other agents or perhaps all of these combined. Agents can be classified as single agent and multi agent systems. Single agent systems consist of a single agent which can interact with resources, humans and other processes to execute a dedicated task. Multi agent systems comprises of set of agents that can interact, cooperate, and coordinate with each other to execute a set of tasks [26]. Software agents are capable enough to solve problems in real world behaving intelligently like humans [27].

Mobile Agent based Network Management (MANM) offers traffic reduction, automation, scalability, robustness with intelligence. In intermittent network connections collaborations are handled efficiently by agent based coordination. Software entities which roam in the network are called mobile agents. The agent takes all the responsibilities of the client node. Each server node have mobile agent to manage and execute in the environment. All the quires are handled by the mobile node. If client needs any service to be accessed it dispatches the mobile agent and does not contact server directly. Once it reaches the server requested service is accessed and it returns back to the client .This elevates the necessity of client node to be connected to network continuously [28].

B. Network environment

The architecture for Vehicular Cloud Network considered is depicted in figure 1. the pool of resources is formed by resources contributed by vehicles, RSU, CSP resources. Two types of communication are used for resources accessing.

- Vehicle-to-Vehicle (V2V)
- Vehicle-to-Infrastructure (V2I)

Resources can be accessed by vehicle nodes from CSP which are spread over large geographical area via RSU. RSU is also responsible for maintaining details regarding vehicle ID's, service taken or given, billing info, SLA's, speed etc.

C. Agency for Trust Evaluation

We present a dynamic trust evaluating agency based on agents, shown in figure 2. It comprise of three types of agents mentioned below.

- TMA-Trust Manager Agent
- TICA Trust Information Collection Agent
- TKB-Trust Knowledge Base

The agency establishes the trust between two communicating entities. The activities conducted by each agent are presented below.

- **Trust Manager Agent (TMA):** It is static in nature and is installed on every vehicle. This agent is responsible for coordinating the activities among the TICA-Information Collection Agent,TKB- Trust Knowledge Base. When a vehicle node requires service the TMA of the vehicle node is triggered. The TMA then activates the TICA to migrate to all neighboring nodes to collect parameters related to trust. Then using the TKB and collected information, the agent calculates the direct and the indirect trust values based on DS theory.
- **Trust Information Collection Agent (TICA):** This agent is mobile and travels around the entire cloud. It visits each neighboring vehicle node to collect trust related information by creating its clones. The clones are the replication of the TICA, but with different destination address. The collected information is updated in TKB in co-ordination with TMA.TMA also utilizes this information to calculate the indirect trust value.
- **Trust Knowledge Base (TKB):** Complete data base related to trust parameters is stored in this

agent. It is static in nature. The information about vehicle ID's, cloud service provider's ID's, bandwidth, Status of the vehicle, list of cloud services provided or requested, SLA, rating ,cost for the service etc. TMA utilizes the information in trust evaluation process.TKB is updated regularly by TMA and TICA.

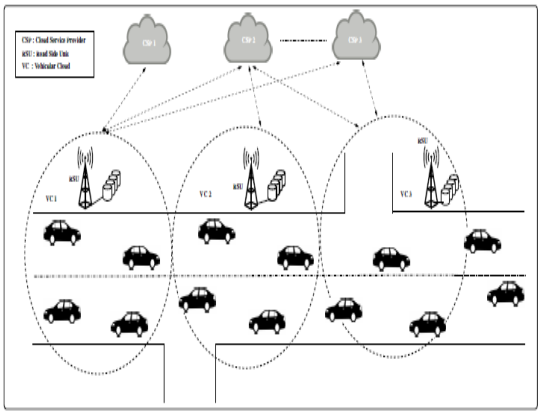

Fig.1. Vehicular Cloud Network

D. Scheme for Trust Evaluation

Proposed agent based trust evaluation scheme works as follows:

- When a cloud user needs service from cloud service provider, TMA of the vehicle node is activated which further triggers TICA. Information about service providers and services rendered by the service providers such as kind of service, duration, cost, Quality of service, etc. related to trust. The collected details are updated at the TMA.
- TMA collects the details from the TICA and TKB. TMA filters the list of service provides and lists only the top ranked service providers along with their respective the trust rating, which match the requirements of the user.

Using the details collected by the TICA and TKB, Direct trust and Indirect trust are evaluated by TMA .The direct trust as stated accounts past transactions which are stored in TKB. The Indirect trust is calculated by using the information collected by TICA. TMA is responsible for the calculation of the cumulative trust using the direct and indirect trust values. Based on the above calculations best cloud service provider is selected by the TMA, which posses all the requirements of the service user and also is highest trust rated.

Each trust value is updated using the DS theory. Dempster Shafer theory is an general form of Bayesian theory of probability which consist of three functions namely basic probability assignment function, belief function, and plausibility function.

Trust value of the service provider and service recipient are updated as given in equation (1).

$$T_{total} = \alpha(TE_{DT}) + \beta(TE_{ID}) \quad (1)$$

α and β are the weights for direct trust and indirect trust respectively which satisfy α + β =1. It is good tendency to assign 'α' a high value, to give more weight for the personal experience of the node than recommendations. The TE_{DT} resembles direct trust and TE_{ID} represents indirect trust. Both TE_{DT} and TE_{ID} are calculated using Dampster Shafer (DS) theory.

Dempster shafer theory can be viewed as a generalization of probability theory. It assumes that fixed entities set which are mutually exclusive as well as exhaustive in nature. The set is represented by θ, which is also known

Assignment function or mass function (m) is defined using equation 2.

$$\sum_{k1 \subseteq k2} \quad m(p) = 1 \quad (2)$$

Where m: $2^{\theta}[0,1]$ and m(ϕ)=0

Unlike the Bayesian theory, the uncertainty is also considered in the DS theory.

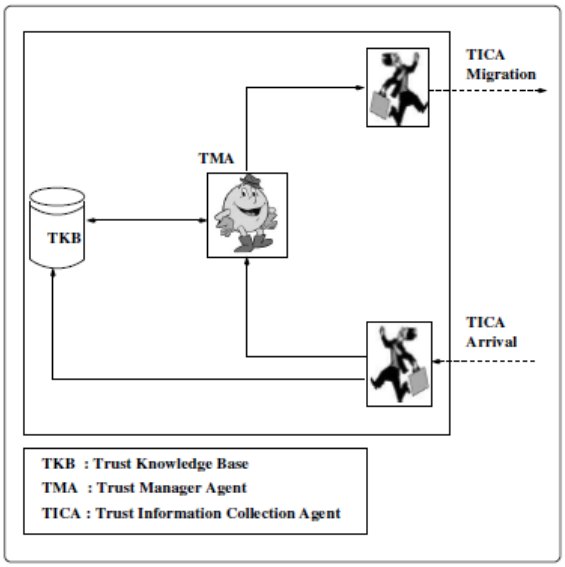

Fig.2. Dynamic Trust Evaluator Agency

as discernment frame. Then BPA *Basic Probability*

Let the frame of discernment for our work be θ = {T, DT}.

Where T represents trust value of TMA towards any attribute.

DT represents distrust value of TMA towards any attribute.

Thus 2^{θ} = {ϕ,{T},{DT},{T,DT}}
where ϕ→ represents a event which is impossible,
{T}→represents level of trust degree,
{DT}→ represents the level of distrust degree and
{T,DT}→represent the level of uncertainty degree.

Then TMA estimates the belief function on the information collected by the TICA as in equation (3).

$$Bel(q) = \sum_{k1 \subseteq k2} \quad m(p) = 1 \quad (3)$$

Where Bel:2^{θ}[0,1]
k1 ⊆ 2^{θ} and k2⊆2^{θ}
where k1 and k2 are sets of relative assertions.

The Plausibility function Pl is expressed as in equation (4) by TMA.

$$Pl(q) = \sum_{k1I\, k1\cap k1\neq 0} \quad m(p) = 1 \qquad (4)$$

Both the belief function and the Plausibility function are two measures of uncertainty. Belief function is the total belief in the set and its corresponding subset. Whereas Plausibility function represents the degree of disapproval or evidence fails. The sum of all Plausibility measures and beliefs need not be equal to one.

1: *Input* : Collection of trust related attributes
2*: Output* : Highest trust rated cloud service provider
3: **Begin**
4: TMA receives trust related information from TICA for different c for each vehicle
5: Calculate the bel and pl respectively for a
6: Calculate the difference between bel and pl
7: **if** *difference is least* **then**
Choose the trust as best .TMA receives the trust related attributes from TKB for different c.
end
8: Repeat step 4 and 5.
9: The bel and pl pair for which the difference is least is the best CSP which the node has interacted (TEID)
10: **End**

Algorithm 1: Algorithm 1

Pl (q)=1- Bel(~q), where ~q is compliment of q.

Bel(~q) is always less compared to Plausibility measures.

As per DS rule of combination, if *n1* and *n2* are two sets of beliefs, then the combination is expressed by TMA as given in equation (5).

$$\sum_{p\cap r=p\neq 0} \quad n1(q)\, n2(r) \qquad (5)$$

Where n1,2(ϕ) = 0;
n1,2(p) = (n1 ⊕ n2)(p) = 1=(1 - K);
and
$K = \sum_{p\cap r=\phi} \quad n1(q)n2(r)$.

The steps involved in evaluation of trust are presented in algorithm 1.

Nomenclature: Number of vehicles - n, Number of cloud service providers - c, Direct trust - TE_{DT} , Indirect trust TE_{ID}, Trust related attributes - a, set of beliefs - bel, Plausibility function – pl.

IV. Simulation

The proposed scheme has been simulated for various network scenarios using C++ language. In this section simulation model, performance parameters, simulation procedure and results are discussed.

A. Simulation model

N Number of vehicle considered for simulation which are moving on fixed road .Length of the road L in Kilometer and breadth B Kilometers. The vehicle can move with the speed range of I to J mts/sec. Each vehicle maintains a minimum safety distance S between each other. Each vehicle node is equipped with a device capable of communicating range of C meters.

B. Performance parameters

The simulation parameters considered to evaluate the performance effectiveness of proposed work are Computational delay, Network configuration time, Total trust evaluation.

- Computational delay: It is defined as the total time taken by the TMA to calculate the Total trust. It is computed in milliseconds.
- Network configuration time: It is the time taken by the network to configure itself. It is computed in milliseconds.
- Total trust evaluation: The sum of direct trust and indirect trust is the total trust value.

C. Simulation procedure

The procedure for simulation of the proposed agent based trust establishment between vehicles in vehicular clouds is as follows.

1: Begin
2: Create cluster and choose cluster head
3: Deploy agent in each vehicle
4: TMA initiates TICA to collect the trust related data from the neighboring nodes
5: TICA submits the collected information to the TMA
6: TMA receives the trust related attributes from TKB for different c
7: TMA evaluates the TEDT and TEID
8: TMA calculates the Ttotal = TEDT + TEID
9: The highest trust rated CSP is selected
10: End

Algorithm 2: Algorithm 2

D. Result analysis

The results obtained for the simulation are presented in this section and are compared with Beta trust scheme. The reasons are: (1) Trust evaluation is based on self experience and other node recommendation (2) Addresses Black hole attack and Grey hole attack.

The time taken for trust evaluation by for different vehicle density under different number of cloud service providers (CSP) is presented in figure 3. As the number of vehicles increases the calculation delay increases

gradually. When the number of cloud service providers are less the trust evaluation is fast, but as the number of cloud service providers increases the evaluation time increases. The reason for this behavior is the amount of trust related information to be collected and evaluated increases with increase in vehicle density and cloud service providers. As the amount of data increases the time taken for trust evaluation also increases. The past experience influence on the trust computation time is shown in figure 4. It shows the variation in computation time of trust with respect to change in number of transactions and number of attributes. As the number of past experiences considered increases along with number of attributes, data for the calculation of trust also increases which gradually increases computation delay. Total trust for different values of α is shown in figure 5. α is the importance factor given to the direct trust and (1- α) is the importance factor of indirect trust. It is observed that as α value increases the total trust calculated is increases by the direct trust value. User can allocate appropriate value for α depending on the amount of influence of direct trust in trust evaluation process.

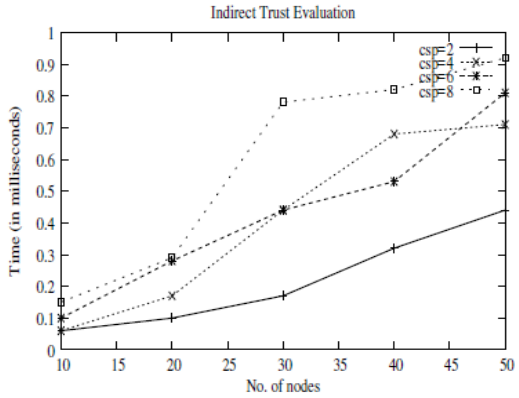

Fig.3. Time versus Number of Nodes

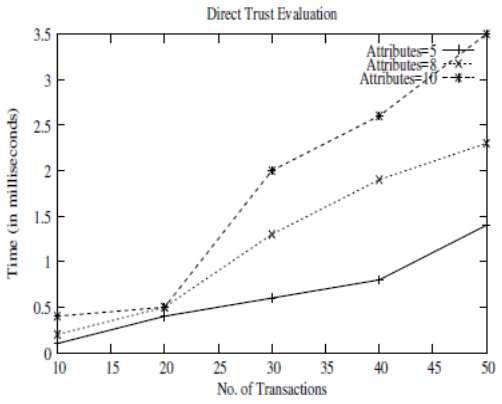

Fig.4. Time versus Number of Transactions

The security threats due to the presence of malicious nodes gaining high trust value are of high risk. The threats mainly include two types of attacks, Black hole attack and ON/OFF attack. Initially the malicious node gain high trust values by successfully sending all the packets they receive. Once a threshold level of trust is attained they start the malicious activities. Because of their high trust value these activities go unnoticed which further create huge damage. In our proposed work the level of damage is decreased considerably. The trust evaluation scheme proposed here decreases the trust value rapidly due to which the malicious node's trust value goes below acceptable level. Trust evaluation for number of interactions is considered in figure 6.

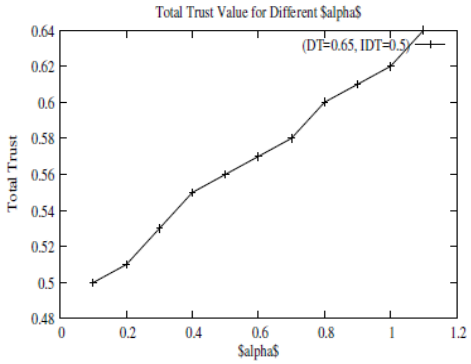

Fig.5. Total Trust versus 'α'

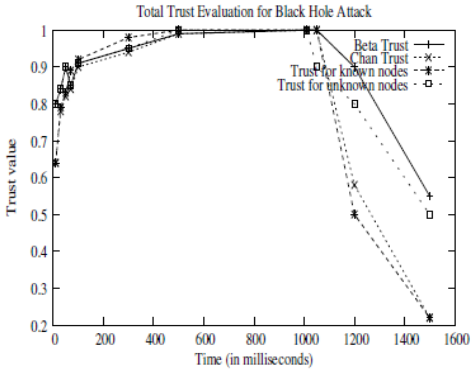

Fig.6. Trust value versus Time (Black hole attack)

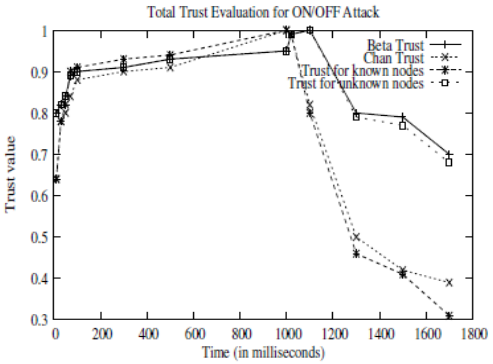

Fig.7. Trust value versus Time (Grey hole attack)

One more kind of attack is the ON/OFF attack. Here the malicious nodes behave either as good or bad opportunistically. This kind of behavior makes it hard for the detection scheme to detect a malicious node and its activities. Having a high trust value they can behave badly and compromise the network. The ON/OFF attack is minimized by the proposed scheme. Trust evaluation for number of interactions is considered in the figure 7. When the malicious nodes start dropping the packets (even in small number) the trust evaluation of the

proposed scheme decreases rapidly for malicious node which makes it easily detectable.

V. Conclusion

Trust between the communicating nodes in Vehicular Cloud is one of the major necessities when dealing with security and privacy. Once an acceptable level of trust is attained, then it will be more feasible to proceed for further connection establishment. In this paper, a frame work is presented for trust establishment which is agent based. The agent establishes trust between cloud service provider and cloud service user using the Dempster Shafer theory. Trust evaluation is based on Personal Opinion, which is evaluated as the direct trust and Recommendation is the indirect trust. To our knowledge trust establishment using software agents and Dempster Shafer theory is a new concept with the advantages of the software agent and the Dempster Shafer theory indulged. The uncertainty in opinion is also considered for the trust evaluation .To test the performance effectiveness of the proposed Trust establishment framework, it has been simulated in C language. Comparison is done with the existing standard methods and our contribution yields good results. Due to rapid reduction in the trust values in our proposed trust evaluation scheme the impact of the malicious nodes is reduced considerably in case of Black hole attack and ON/OFF attack.

References

[1] R. Hussain, J. Son, H. Eun, S. Kim and H. Oh, ”Rethinking Vehicular Communications: Merging VANET with cloud computing,” 4th IEEE International Conference on Cloud Computing Technology and Science Proceedings, Taipei, 2012, pp. 606-609.

[2] R. Kaur, T. P. Singh and V. Khajuria, “Security Issues in Vehicular Ad-Hoc Network (VANET),” 2nd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, 2018, pp. 884-889.

[3] P. Mell, “What’s Special about Cloud Security?,”in IT Professional, vol. 14, no. 4, pp. 6-8, July-Aug. 2012.

[4] V. Marbukh, “Systemic Risks in the Cloud Computing Model: Complex Systems Perspective,” IEEE 9th International Conference on Cloud Computing (CLOUD), San Francisco, CA, 2016, pp. 863-866.

[5] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun and Y. Xiang, ”Block Designbased Key Agreement for Group Data Sharing in Cloud Computing,” in IEEE Transactions on Dependable and Secure Computing.2017

[6] K. Naseer Qureshi, F. Bashir and S. Iqbal, “Cloud Computing Model for Vehicular Ad hoc Networks,” 2018 IEEE 7th International Conference on Cloud Networking (CloudNet), Tokyo, 2018, pp. 1-3.

[7] N. Hegde and S. S. Manvi, “Thesis Proposal Summary: Key Management Authentication and Non Repudiation for Information Transaction in Vehicular Cloud Environments,” 2016 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), Bangalore, 2016, pp. 157-160.

[8] G. Yan, D. B. Rawat and B. B. Bista, “Towards Secure Vehicular Clouds,” 2012 Sixth International Conference on Complex, Intelligent, and Software Intensive Systems, Palermo, 2012, pp. 370-375.

[9] Soleymani, Seyed Ahmad, Abdullah, Abdul Hanan, Wan Haslina, Anisi, Mohammad Hossein, Goudarzi, Shidrokh, Rezazadeh Baee, Mir Ali, Mandala, Satria. “Trust management in vehicular ad hoc network: a systematic review”, EURASIP Journal on Wireless Communications and Networking, Vol. 2015, No. 1, pp. 146, 2015.

[10] Noor, Talal H., Sheng, Quan Z., Zeadally, Sherali, Yu, Jian, “Trust Management of Services in Cloud Environments: Obstacles and Solutions”, ACM Computing Surveys (CSUR), Vol. 46, No. 1, pp. 12-30, July 2013.

[11] R. Kaur, T. P. Singh and V. Khajuria, “Security Issues in Vehicular Ad- Hoc Network(VANET),” 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, 2018, pp. 884-889.

[12] R. Hussain, J. Son, H. Eun, S. Kim and H. Oh, “Rethinking Vehicular Communications: Merging VANET with cloud computing,” 4th IEEE International Conference on Cloud Computing Technology and Science Proceedings, Taipei, 2012, pp. 606-609.

[13] Deeksha, A. Kumar and M. Bansal, “A review on VANET security attacks and their countermeasure,” 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC), Solan, 2017, pp. 580-585.

[14] Z. M. Aljazzaf, M. Perry and M. A. M. Capretz, “Towards a unified trust framework for trust establishment and trust based service selection,” 2011 24th Canadian Conference on Electrical and Computer Engineering (CCECE), Niagara Falls, ON, 2011, pp. 001175-001178.

[15] S. Ahmed and K. Tepe, “Evaluating trust models for improved event learning in VANETs,” 2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE), Windsor, ON, 2017, pp. 1-4.

[16] D. Saraswat and B. K. Chaurasia, “AHP Based Trust Model in VANETs,” 2013 5th International Conference and Computational Intelligence and Communication Networks, Mathura, 2013, pp. 391-393.

[17] Y. Wei and Y. Chen, “Adaptive decision making for improving trust establishment in VANET,” The 16th Asia-Pacific Network Operations and Management Symposium, Hsinchu, 2014, pp. 1-4.

[18] R. Kaur and J. Kaur, “Cloud computing security issues and its solution: A review,” 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2015, pp. 1198-1200.

[19] S. Sasirehka, S. Vijayakumar, K. Abinaya, “Unified trust management scheme that enhances the security in MANET using uncertain reasoning”, International Conference on Electronics and Communication Systems (ICECS), pp. 1497-1505, 2015.

[20] K. Sharma, B. K. Chaurasia, “Trust Based Location Finding Mechanism in VANET Using DST”, Fifth International Conference on Communication Systems and Network Technologies, pp. 763-766, April 2015.

[21] B. Yang, R. Yamamoto, Y. Tanaka, “Dempster-Shafer evidence theory based trust management strategy against cooperative black hole attacks and gray hole attacks in MANETs”, International Conference on Advanced Communication Technology, pp. 223-232, February 2014.

[22] Gayathri Dhananjayan,Janakiraman Subbiah, “T2AR: trust-aware ad-hoc routing protocol for MANET”, http://springerplus.springeropen.com/articles/10.1186/s40 064-016- 2667-6, 2016.

[23] Taroun, Abdulmaten and Yang, Jian-Bo. “Dempster-Shafer Theory of Evidence: Potential usage for decision

making and risk analysis in construction project management",The Built 'I&' Human Environment Review. Vol. 4.2011.
[24] M. S. Kakkasageri, S. S. Manvi, Jeremy Pitt, "Cognitive Agent Based Critical Information Gathering and Dissemination in Vehicular Ad hoc Networks", Wireless Personal Communications, Vol. 69, No. 4, pp. 1107- 1129, 2013.
[25] Ritu, S. Jain, "A trust model in cloud computing based on fuzzy logic", IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT), pp. 47-52, May 2016.
[26] M. S. Kakkasageri and S. S. Manvi, "Safety information aggregation in VANETs using vehicle beliefs," 2011 Fifth IEEE International Conference on Advanced Telecommunication Systems and Networks (ANTS), Bangalore, 2011, pp. 1-6.
[27] A. Leite, R. Girardi and P. Novais, "Using Ontologies in Hybrid Software Agent Architectures," 2013 IEEE/WIC/ACM International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT), Atlanta, GA, 2013, pp. 155-158.
[28] M. K. Kona and Cheng-Zhong Xu, "A framework for network management using mobile agents," Proceedings 16th International Parallel and Distributed Processing Symposium, Ft. Lauderdale, FL, 2002,
[29] Y. Wei and Y. Chen, "Adaptive decision making for improving trust establishment in VANET," The 16th Asia-Pacific Network Operations and Management Symposium, Hsinchu, 2014, pp. 1-4.

Authors' Profiles

Shailaja S. Mudengudi completed her B. E in electronics and communication engineering from Visvesvaraya Technological University Belgaum, India and M.Tech in Digital Electronics and Communication from Visvesvaraya Technological University Belgaum, India. Presently, she is working as Assistant Professor in Department of Electronics and Communication Engineering, Tontadarya College of Engineering , Gadag, Karnataka India. She has published 1 international conference paper. Her areas of interest are wireless networks,MANET's,VANET's, and sensor networks.

Dr. Mahabaleshwar S. Kakkasageri received his B. E. Degree from Karnataka University, M. Tech degree in Digital Communication and Ph.D. degree from the Visvesvaraya Technological University, Belgaum, Karnataka, India. He has experience of 15 years in teaching. His research interests are: Vehicular Ad hoc Networks, Software Agent based Network Management, Wireless Networks, and Internet of Things. He has published 40 papers in national and international conferences, 15 papers in national and international journals, and 03 publications/books/books chapters. He is a member of IETE. He is a reviewer and programme committee member for many journals and international conferences, respectively. He received Seed Money to Young Scientist for Research from VGST Karnataka in 2015.

How to cite this paper: Shailaja S. Mudengudi, Mahabaleshwar S. Kakkasageri, "Agent Based Trust Establishment between Vehicle in Vehicular Cloud Networks", International Journal of Computer Network and Information Security(IJCNIS), Vol.11, No.7, pp.29-36, 2019. DOI: 10.5815/ijcnis.2019.07.05