Volume 3, Issue 5
October 2014

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

©2012-13 International Journal of Information Technology and Electrical Engineering

TRUST Levels in Vehicular Adhoc Network (VANET)

Irshad Ahmed Sumra[1], Halabi Bin Hasbullah[2]
[1,2]Computer and Information Sciences Department
Universiti Teknologi PETRONAS, Bandar Seri Iskandar, 31750, Tronoh, Perak, Malaysia.
[1]isomro28@gmail.com, [2]halabi@petronas.com.my

Jamalul-lail Ab Manan[3]
[3]Advanced Information Security Cluster, MIMOS Berhad
Technology Park Malaysia Kuala Lumpur, Malaysia.
[3]jamalul.lail@mimos.my

ABSTRACT

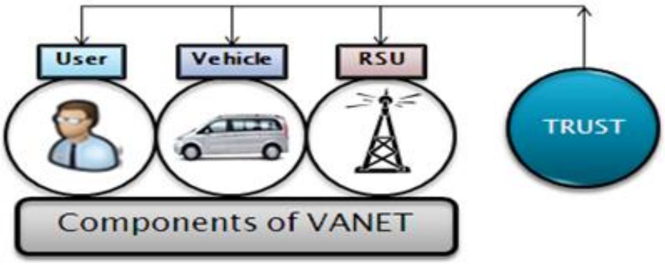
Content based applications and lifesaving applications running in vehicular network are attracting more end users to use them. However, there are several pertinent issues especially those related to lifesaving applications. Security and trust are the main stumbling blocks. Entities such as users, vehicles and Road Side Units (RSUs) need accurate and timely information to carry out their activities normally. In this paper we present some of our findings with regards to the behaviour of entities in Vehicular Ad hoc Network (VANET). We noted that in a more serious attack scenario, any one of the entities could change their behaviour. A legitimate user, for example, may change suddenly from a normal user to become an attacker. In this paper, we propose three different trust levels for VANET to enable us to precisely categorize and determine all entities within the network. A legitimate user that has become an attacker would change its existing trust level and its trust relationship with the rest of the entities in network due to its change of behaviour. Our objective is to achieve quick decision on what to do based on trust levels by the VANET entities whenever something suspicious happening and change of behaviour of any entity. Hence, by monitoring trust levels of its neighbours, each entity in VANET can assist in preventing attacks in the network.

Keywords: *Security, Trust, Safety and non-Safety applications, Attacker, Trusted user, Behaviour, Malicious User, Trust levels.*

1. INTRODUCTION

Vehicular network applications are expected to be safe because one of the major concerns in the network is security. As such, users of these applications expect to receive correct and trustworthy information during their journey. This is because trust is a major factor in security; therefore, trust must be inherent in the system, in all the elements in the information infrastructure (RSU). Users, vehicles and road side units (RSUs) make up the major elements of trusted vehicular network which are expected to act accordingly. A sudden alteration from the normal actions in any of these elements of the infrastructure could mean that the network is no longer trustworthy. To explain the meaning of trust, a definition in related literature is provided as follows. Presented here is the idea of trust in MANET [1].“*The trust of a particular node is a subjective assessment by an agent/other peer node on the reliability and accuracy of information received from or traversing through that node in a given context. Trust reflects the belief or confidence or expectations on the honesty, integrity, ability, availability and quality of service of target node’s future activity/behaviour. It also reflects the mutual relationships where a given node behaves in a trustworthy manner and maintains reliable communications only with nodes which are highly trusted by the given node”.* Trust in a

VANET is viewed in this way, “*all components (User, Vehicle, and RSU) of network should behave in an expected manner and serve the user*”. RSUs, users and vehicles are all active elements involved in a trusted vehicular network and as such they are required to act in a way that is anticipated during the time that they are transmitting and receiving both safety and non-safety messages. The user, vehicle and RSU some of the main components of vehicular network and play two roles as elements of vehicular communications; they are the roles of trustee and trustor. This is presented in Figure 1, where the trusted communication in a vehicular network is explained. Every components of vehicular network behave in a proper manner and we can achieve the trust in vehicular network. If any components of the network change its behaviour then level of trust will be affected.



©2012-13 International Journal of Information Technology and Electrical Engineering

Figure 1. TRUST with component of VANET

This paper has been divided into the following five sections: Section 2 discusses in details the major components of trust in vehicular network. Related work in the field of trusted vehicular communication is discussed in detail in Section 3. Three trust levels for a vehicular network are proposed in Section 4; each level will be described by way of some formal definition. Finally, the conclusion and future work is given in Section 5.

2. TRUST COMPONENTS IN VANET

There are three components of vehicular TRUST which are mentioned in Figure 2, and each component has its own important role for building a trusted communication environment. Next, each component and its possible functionality in a vehicular network are discussed in detail.

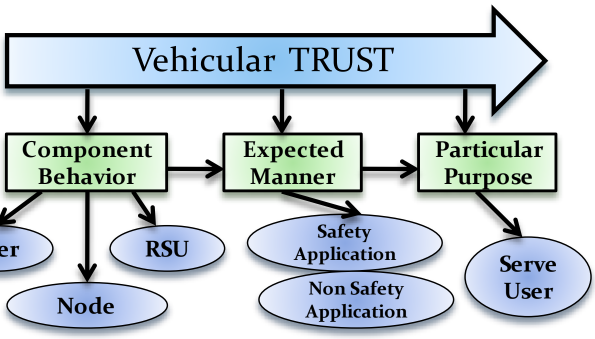


Figure 2. Components of Trust in VANET

1. First Part of Trust - Component Behaviour

The following show three kinds of behaviours of components in a vehicular network.

a) User Behaviour (UB): The most important component in the entire communication environment is the user in achieving the different levels of trust by which an environment can be secured. The relationship of a user with the various components of a network is shown in Figure 3.

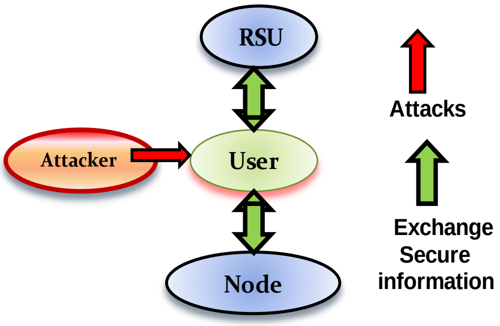


Figure 3. User relationship with different entities in network

- Types of User Behaviours

A user has a dynamic behaviour and changes his/her behaviour according to the information received from other users or from the roadside unit (RSU). There are two types of user behaviour.

- Positive Behaviour
- Negative Behaviour

Positive Behaviour: A user receives a warning message from another user or from the RSU, and then changes his/her behaviour according to the content of the message and also forwards this message to other users of the network. This reflects the positive behaviour of the user and on the basis of behaviour, users can be divided into two types.

i. Trusted Users (TUs)

ii. Non-Trusted Users (NTUs- Attackers)

Trusted Users (TUs) are those who perform their task properly in the network. The behaviour of a trusted user may change upon receiving messages from other vehicles or from the RSU. When a trusted user receives an accident warning or traffic jam message, the user is expected to change his/her behaviour, that is, slow down his/her vehicle or change route. Figure 4 describes the situation in which vehicle C sends a warning message to other vehicles (D, E). As a result, the users of vehicles D and E slow down their speeds and may take an alternative route due to the accident warning message.

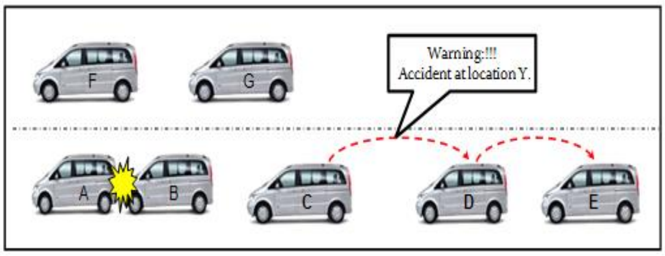


Figure 4. Trusted User Behaviour

Negative Behaviour of Non-Trusted Users (Attackers): Attackers are those who intentionally create problems for users in a network by launching different types of attacks (passive or active). In a vehicular network, they become more prominent because they can potentially change a critical message or broadcast a wrong message to other vehicles. Figure 5, explains an example whereby attacker X sends a message (Hello!!! You are an idiot) to vehicle B and this message changes the behaviour of user B. User B might become upset and increase the speed of his/her vehicle and this would pose a problem for other users.

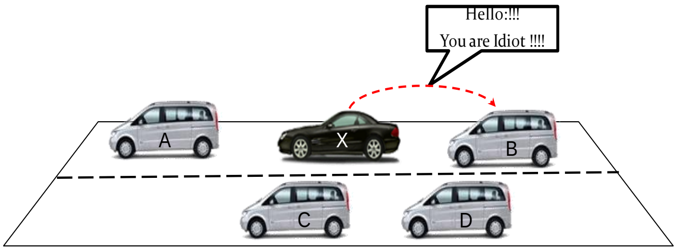


Figure 5. Attacker behaviour through social Attack

b) Vehicle (Node) Behaviour

The vehicle (Node) is also another key communication aspect of the vehicular network and it comprises a combination of hardware and software. A smart node is a combination of

different types of embedded sensors (autonomous sensors (AS) and cooperative sensors (CS)), and processing and communication ability modules. A Data Recorder (EDR), Tamper Proof Device (TPD), Trusted Platform Module (TPM), Global Position System (GPS), Radar Systems (RSs), Communication Facility (CF), Computing Platform (CP), and a
Human Machine Interface (HMI) are some of the modules [9] that are used inside the smart vehicle. The On-Board-Unit (OBU) is the main communication module that resides inside the vehicle and provides communication with OBUs of other vehicles and also with RSU. The purpose of this module is to send and receive messages in network. The Application Unit (AU) works inside the vehicle and sends and receives safety and non-safety application messages in the network. Electronic Control Unit (ECU) and other types of sensors work inside the vehicle and it is necessary for all of the modules of vehicle to work in an expected manner. If the software or the hardware of a vehicle changes its behaviour due to an attack on the infrastructure, then it would be difficult for users to carry on with their journey on the highway. Malicious users can send malicious programs while communicating with other users or with the roadside unit (RSU), such as Trojan horse or other viruses, which could create trust issues for the users.
For example, if the RSU is affected by an attacker and legitimate users send a request for a software update, the user could end up downloading a malicious program instead of updating their software. Figure 6 explains this situation in a network.

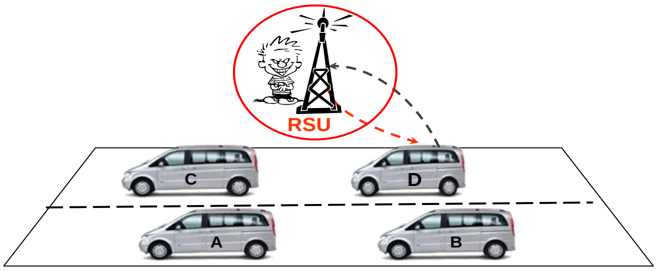


Figure 6. Malicious software downloaded from RSU to vehicle

c) Road Side Unit (RSU) Behaviour
Infrastructure (RSU) plays a vital role in a vehicular network whereby the RSU verifies the users and provides the right information on road. Due to attacks, RSUs may also change their behaviour by sending wrong messages in the network. This should not happen if the infrastructure is trusted and all users can rely on it.
Figure 7, explains the scenario whereby an attacker communicates with the RSU and broadcasts one wrong warning message to a group of users (A, B, C and D) on the highway.

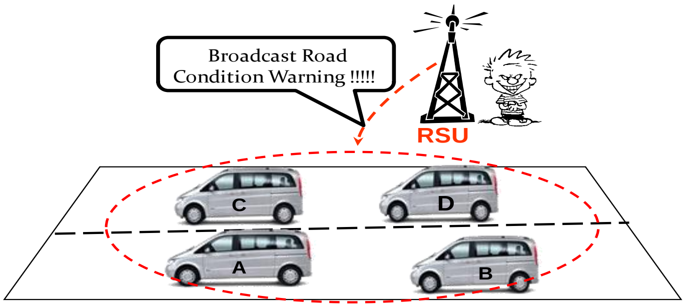


Figure 7. RSU broadcasts wrong message

2. Second Part of Trust - Expected Manner

"The trustor entity not only believes the trustee will behave in an expected manner but also is willing to be vulnerable for that belief in a specific context, i.e., trustor is willing to assume the risk that the trustee may not behave as expected"[90].

A user expects other users and also the RSU to behave in an expected manner and send the right messages while communicating with them. A user also expects to receive safety and non-safety messages generated from source. The integrity of the data is expected be maintained by users, vehicle and RSU and all the entities are expected to perform their task accurately. Where vehicular trusting communication is concerned, the trustor entity (vehicle or RSU) must believe that the trustee behaves as expected and according to the competence and goodwill of the trustee entity. This is one of the most recognized aspects of trust in communication between the different entities of a network.

3. Third Part of Trust - Particular Purpose

The purpose of building trust in the components of vehicular network is to serve users via its potential safety and non-safety applications. If users are not properly served via these applications, then trust has not been established in the network. Active safety applications, warning applications and position-based routing require protection against attackers and if an attacker changes the messages related to these applications, it will affect the behaviour of the end user. Applications should behave as expected because a user makes decisions based on the behaviour of these applications. When all entities of the network behave in the expected manner, it will increase the level of trust between them and consequently, secure the vehicular communication.

3. RELATED WORK

M.Gerlach et al. [2] suggested a model for trusted applications for VANET. They described a situation where the characteristics of trust that are pertain to the trustee. The authors mentioned three key contributions which are given below.

- Proposed a security architecture that is integrated with various security measurements in vehicular environments.

- Proposed a trusted model for applications in VANET by utilizing trust tagging principle.
- Proposed the idea of mixed content and defines the manner by which pseudonyms can be changed which prevents location tracking.

T.Chen et al. [3] proposed a trusted routing framework, which allow authentication of messages, establishment of node to node trust and verification of routability, without the need for online Certificate Authorities (CA). This particular method prevents identity impersonation, which suggests that links are available if they are false, and some other specific invalid routing protocol actions. The trusted routing framework has been used with the Optimized Link State Routing Protocol (OLSR) and has shown the manner by which trusted routes can be created using this application. An established trust framework is made up of three main components, which have been created to deal with various types of threats in the network.

- A digital signature is utilized to authenticate messages. The specific digital signature value is dependent upon secret values, to which only the original signer is privy to.
- The hash function creates and signs a fixed size message digest in place of the complete message.
- Vehicle to Vehicle authentication is another component of the trusted routing, that authenticates a vehicle with another vehicle, and protects it from any and all would be attackers.

J. Cui et al. [4] proposed a new trusted routing scheme for reliable communication to provide reliable packet delivery in a VANET. The author used the idea of similar characteristics to search for nodes that are possibly friendly from among the many unknown nodes. They proposed a forwarding rule based on this idea which calculates resulting attribute similarity value. The effectiveness of this scheme in selecting more trustworthy routes and protecting against malicious components as compared with the DSR protocol has been validated by the simulation results. A summary of their contributions is given below:

- Proposed a method in evaluating trust in regards to forwarding packets is a scheme based on the idea of the similarities of attributes.
- Proposed an approach to calculate the attribute similarities between two specific nodes.
- Proposed a rule used for packets to be forwarded, such as practical behaviours.
- Proposed a method by which the similar attributes can be incorporated into the DSR protocol in order to enhance the delivery of packets.

P. Wex et al. [5] discussed some issues of trust in vehicular networks. The general belief is that every component in a vehicular environment possesses its own system of trust, which can make decisions about which components can be trusted. Below are the two basic options for establishing trust.

- Statically: By the static dependence on a security infrastructure.
- Dynamically: By the dynamic build-up of trust in a way that is self-organizing.

✓ Infrastructure-based Trust Establishment: there are various methods used to establish infrastructure-based trust. In principle, Infrastructure based Trust Establishment utilizes certificates to build this trust and is static over time.

✓ Self-organizing Trust Establishment: VANET is very dynamic, and hence need a style of trust establishment that is very adaptable; i.e. decisions related to the trustworthiness of other components must be autonomous due to that fact that there is no possible connection to an online security infrastructure. In principle, Self-organizing Trust Establishment is achieved on the basis of incomplete data, which has been collected from unknown components over a limited amount of time while communicating among the components in the network.

X. Hong et al. [6] proposed a trust architecture and model called Situation-Aware Trust (SAT). This model deals with several important trust concerns present in vehicular networks. Among the contributions are the following:

- Proposed an efficient policy management for a wide variety of situations by utilizing cryptographic solutions, which are based on descriptive attributes.
- Proposed both off-line and on-line trust policies and requirements which are built for pro-action and prediction of future trust situations.
- Transformed the trust established in Internet social communities to VANET for enhancement and promotion of VANET applications.

J. Serna et al. [7] proposed a privacy solution which was designed on the basis of two principles, i.e. Mandatory Access Control and Geolocation-based Trust Propagation. The Geolocation based trust propagation portion makes use of a PKI infrastructure and allows end users (vehicles in the VANET) carry out the process of authentication in domains that are not trusted by providing dynamic interoperability among various CAs having no clearly expressed agreement. In such environment they suggested utilizing a trusted third party that can provide authentication of digital certificates by distributing access credentials, which can be used for purposes of authorization.

S. Mazilu et al. [8] proposed a data-trust security model and designed social network theories for vehicular network. Proposed model computes a trust index for each message based on the relevance of the event. Among their contributions are given below.

- Proposed a solution to the security problem using social network theories.
- Evaluated the proposed solution by modelling and simulation.
- Claimed that the data-trust security model had successfully prevented attacks (message alteration) in VANET.

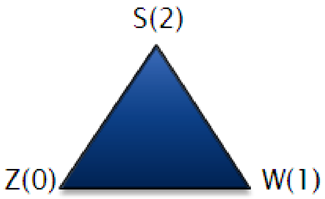
©2012-13 International Journal of Information Technology and Electrical Engineering

In our previous work [9], we proposed three trust levels and also explained the Trust components in vehicular network. So in this paper, we are extending our previous work.

4. PROPOSED TRUST LEVELS

Vehicular networks have many entities which are supposed to act in an anticipated way to garner the necessary trust among them. We propose three trust levels here. An assessment of the role of the negative users (attackers) and the positive users in the vehicular network has been given to each specific level. The three trust levels in the vehicular network are shown in Figure 9 along with the corresponding trust entity values.

Definition: Trust (e, l, a)

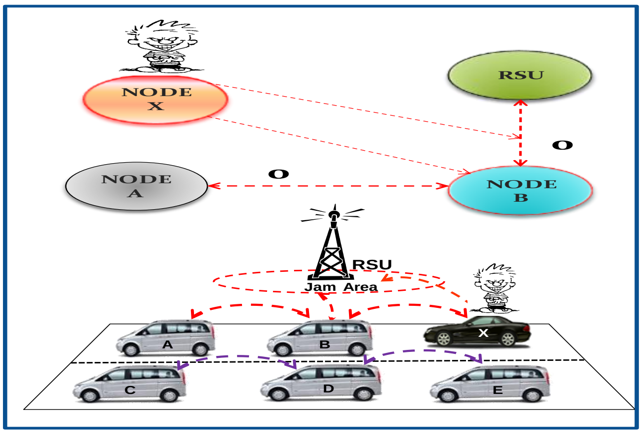


$$e \in [n, u, r]$$
$$l \in [0, 1, 2]$$
$$a \in [-, +]$$

Figure 9. Proposed Trust Levels

A) Zero Trust (Z0)

The first level of trust is known as Zero Trust. Here, the attacker is domineering and other users of the network are unable to communicate or access any of the services in the network; this is because of the various attacks being created by the attacker. In short, we can say there is no communications in network, which means that the trust value for sending and receiving is zero due to a specific attack e.g. DoS attack. Figure 10, shows a scenario whereby attacker X launches a DoS attack and jams the whole communication medium between vehicle-to-roadside (V2R) communications. Vehicle B is not able to access services form the roadside unit (RSU). Attacker X also drops communication packets of vehicle B and in doing so, the whole network is affected due to the negative behaviour of the attacker.

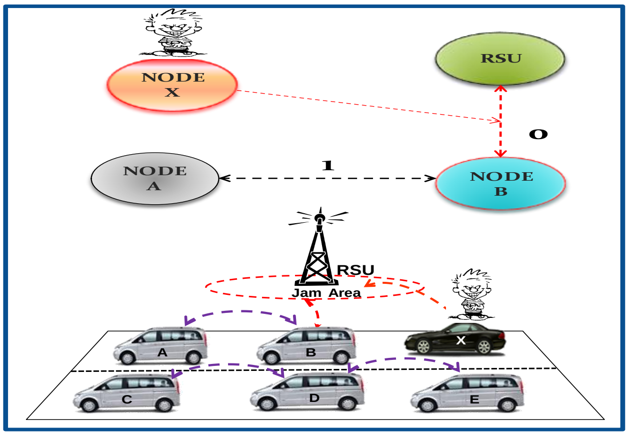


- Trust (A, B, L0, X (-))
- Trust (A, R, L0, X (-))
- Node A and node B has zero Trust relationship because there is no communication (action) between these two nodes.
- Node A and roadside unit R has zero Trust relationship because there is no communication between these two entities of network.

Figure 10. Zero Trust Levels

B) Weak Trust (W1)

The second trust level is known as the Weak trust. This situation is where various types of attacks are launched by an attacker but only in a specific area. In this situation only some entities are bothered by the attacks; some of the entities of the network are unaffected by the attacks and can continue to serve the users of the network and perform their duties correctly. Figure 11, describes the scenario in which node B is not able to make communication with roadside unit (RSU) but is able to communicate with node A.

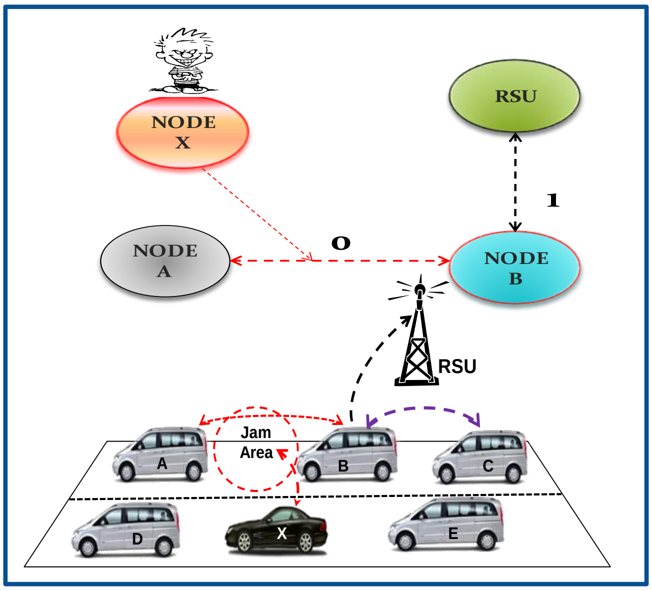


- Trust (A, B, L1, A ↔ B, +)
- Trust (B, R, L0, X (-))
- Node A can communicate with node B, but node B cannot communicate with roadside unit (RSU) due to attack. So finally the node B has weak trust level in network.

Figure 11. Weak Trust (a)

Figure 12 explains the second scenario in which the node B can communicate with the roadside unit (RSU) but the vehicle-to-vehicle (V2V) communication is disturbed due to a DoS attack. However, node B cannot communicate with node A due to a DoS attack.

©2012-13 International Journal of Information Technology and Electrical Engineering



Trust (B,R, L1, B ↔ R, +)

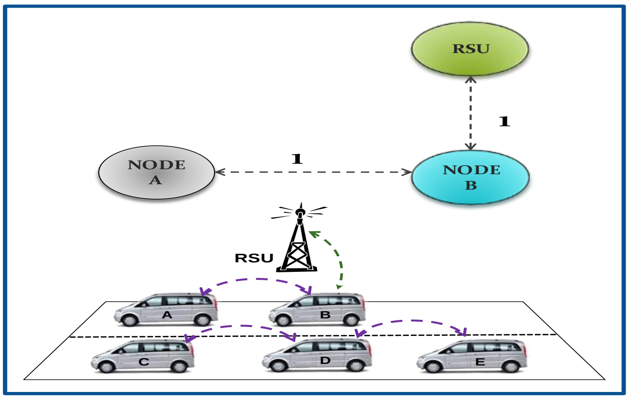
Trust (A, B, L0, X (-))

- Node B can communicate with roadside unit (RSU), but node B cannot communicate with node A due to attack. So finally, level of trust of node B is weak trust in network.

Figure 12. Weak Trust (b)

C) Strong Trust (S2)

When every entity in a network performs his/her/its duties correctly and is therefore trusted, it is known as strong trust. This is a perfect situation as no attackers are present in the network and each entity carries out his/her/its duties correctly. Figure 13, shows the strong trust levels in which node B performs all types of tasks and uses all types of services from other nodes and also from the RSU.



- Trust (A, B, L2, A ↔ B, +)
- Trust (B, R, L2, B ↔ R, +)
- *Node B has strong Trust relationship with node A and also with RSU. Node B can communicate with other components of network (vehicle, RSU).*

Figure 13. Strong Trust

Entity (e) – stands for any of the following: an RSU (r), a node (n), and a User (u); in a vehicular network, these are the three main entities.

Trust Level (***l***) - stands for the trust levels among the entities of the network. The possible degrees of trust are Zero Trust (ZT), Weak Trust (WT) and Strong Trust (ST).
Action (***a***) - stands for what the user is doing during the time they are communicating in the network. If the user in the vehicle to (RSU) or vehicle to vehicle communication sends messages that are accurate, they will be given a positive value (+). So, the role of the user is considered to be positive and all of his/her communication in the network is trusted.
However, if a user should suddenly alter his/her actions by sending false messages or disrupt communication, he or she is considered an attacker; a negative value (-) will then be given to the user who is no longer trustworthy. The Figure 14 describes the trust definition for three trust levels (zero, weak and strong) with different examples.

Table.1 explains the three different types of trust levels with trust conditions and description of trust in vehicular network. The three elements of trust are defined in this definition.

Table I. Trust levels with its conditions and description

Trust Level	Trust Conditions	Trust Description	Trust and Attackers
0	Send NOT Receive	Zero Trust (Z0)	Attacker and attack are part of the network, user, vehicle and RSU did not work properly due to attacks.
1	Send OR Receive	Weak Trust (W1) (Some Entities are Trusted)	Attacker is part of the network, but some entities are affected due to attacks.
2	Send AND Receive	Strong Trust (S2) (all Entities are Trusted)	There is no attacker in network and all entities of the network are trusted.

The following three cases show the relationship of an attacker with the level of Trust in a network. Figure 15, explains the relationship of attackers and attacks with different levels of trust in a network.
Case A: The user performs all the tasks of the vehicular network as well as uses safety and non-safety applications. Sending and receiving is both possible and the user is enjoying his/her journey with all the potential applications of the vehicular network. There is no role of attacker in the network and so, a strong trust grade will be assigned to this particular user.
Case B: In this case, there are two different scenarios as described below:

©2012-13 International Journal of Information Technology and Electrical Engineering

- In the first scenario, an attacker only conducts a traffic analysis of the network users. This attack is more concerned with privacy. However, the attacker remains part of the network and he/she sends and receives tasks accurately.
- In the second scenario, an attacker alters safety or non-safety messages that are received by other users. However, the attacker is still part of the network and performs the tasks of sending and receiving in the network.

Case C: Availability is one of the key security requirements of a network; the network should be available in any condition and the users must perform their tasks accurately. A DoS attack is one of infamous attacks that directly affects the level of trust in a network. Whenever an attacker jams the communication medium, users can no longer be part of the network. This is a serious condition as whenever a user needs to pass messages (safety and non-safety) to other users of the network, there is no network service available. In this condition, the level of trust becomes zero. The objective of this study has been to reduce the role of attacker and their attacks in network, and to achieve the maximum level of Trust in a network.

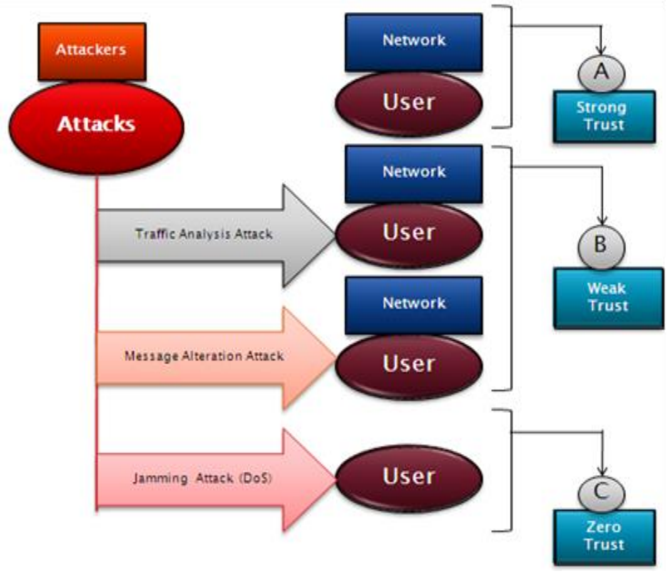


Figure 15 Relationships of Attacker and Attacks with Trust Levels

Figure 16, describes the scenario in which the city area has been divided into different zones and user A finds different trust levels in different zones along his journey. The objective of these trust levels is to find the degree of trust in the vehicular network and also to find the behaviour of attackers and attacks in different parts of network. The City area is divided into three parts.

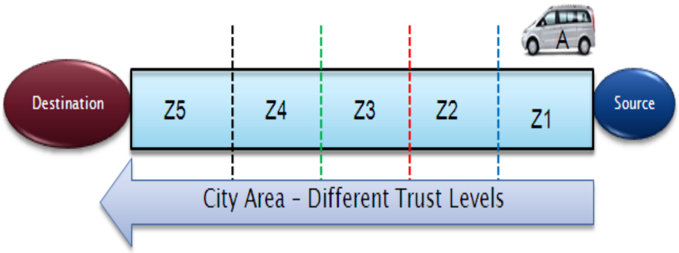


Figure 16 Different Trust levels for user A in the city area

- Zero Trust Area (ZTA): Users in this area remain part of the network but are not able to access network services due to DoS attack and the trust level here is considered zero.

- Weak Trust Area (WTA): Here are three possible cases:
  - The user is part of the network but he/she receives wrong messages from other users (attackers) of the network.
  - Vehicle-to-vehicle (V2V) communication is possible but vehicle-to-roadside unit (V2R) communication is not possible due to attack.
  - Vehicle-to-roadside unit (V2R) communication is possible but vehicle-to-vehicle (V2V) communication is not possible.

- Strong Trust Area (STA): This is an ideal situation in which the user sends and receives all kinds of messages in vehicle-to-vehicle (V2V) and also vehicle-to-roadside unit (V2R) communication. User is well-connected with all the components of the network and sends and receives safety and non-safety messages. There is no attacker in this situation and all components of the network are working properly. This is an ideal condition and for the successful implementation of vehicular network, it is necessary to achieve strong trust in the network.

Some Possible Conditions for TRUST Levels

Here we are mentioning some possible conditions that are related to trust levels; these conditions are actually types of DoS attacks [10], so we directly relate these attacks with trust levels and explain it which attack affected the levels of trust in vehicular network. There are following conditions to assign the Trust levels.

a. Drop the Communication Packets: This is a feature related to the behaviour of attackers where an attacker does nothing but drop packets; the goal of the attacker is to make sure that users are unable communicate in the network in any way.

b. Overwhelm Network Resources: In this attack, the attacker aims to overwhelm the resources of the user's vehicle in order to hinder its performance of other necessary tasks. The access signals of the vehicle's network become overly busy and this uses up all its resources in trying to verify the messages.

c. Jammed Communication Channels: In this attack, high frequency signals are sent out by the attacker that causes the communication channel between vehicles to be jammed. As a result the vehicles are unable to send or receive safety or non-safety messages in network. No services are available in that particular domain because of this attack and only upon leaving that domain will they receive the messages.

5. CONCLUSION AND FUTURE WORK

This paper has presented trust levels as a way to increase the security of VANETs. When entities of the network such as other users, vehicles or RSUs act in a way that is as anticipated, the users will be served well by the applications in the vehicular network, whether they are related to safety or non-safety messages. However, the situation can become dangerous for legitimate users of the network if any entity suddenly change its behaviour to become an attacker. In this paper, we have presented three trust levels in vehicular network to enable entities monitor its neighbours' trust levels so that any sudden change in behaviour such as an attack can be prevented. We will present simulation experiments in future work to precisely simulate varying situations according to trust levels, whenever changes happen within the network and predict potential attacks and warn legitimate users to avoid attacks in VANET.

ACKNOWLEDGEMENT

This work is supported by Universiti Teknologi PETRONAS (UTP) Postgraduate Assistantship Scheme with collaboration of MIMOS Berhad.

REFERENCES

[1] R. Shankaran, V. Varadharajan, M. A. Orgun, and M. Hitchens, "Context-Aware Trust Management for Peer-to-Peer Mobile Ad-Hoc Networks", 33rd Annual IEEE International Computer Software and Applications Conference, 2009.

[2] M.Gerlach, F. FOKUS, "Trust for Vehicular Applications" IEEE Computer Society, Proceedings of the Eighth International Symposium on Autonomous Decentralized Systems, p: 295-304, year of publication: 2007.

[3] T.Chen, O.Mehani and R.Boreli, "Trusted Routing for VANET" 9th International Conference on Intelligent Transport Systems Telecommunications (20 October 2009), pp. 647-652.

[4] C. Jingwen, G. Qiang,, "A novel trusted routing scheme using attribute similarity for VANET", Advanced Computer Control (ICACC), 2011 3rd International Conference.

[5] P. Wex, J. Breuer, A. Held, T. Leinmuller, L. Delgrossi, "Trust Issues for Vehicular Ad Hoc Networks," Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE , vol., no., pp.2800-2804, 11-14 May 2008.

[6] D. Huang; X. Hong; M.Gerla, "Situation-aware trust architecture for vehicular networks," Communications Magazine, IEEE , vol.48, no.11, pp.128-135, November 2010.

[7] J. Serna, J. Luna, M. Medina, "Geolocation-Based Trust for VANET's Privacy," Fourth International Conference on Information Assurance and Security, 2008. ISIAS '08., pp.287-290, 8-10 Sept. 2008.

[8] S. Mazilu, M. Teler, C. Dobre, "Securing Vehicular Networks Based on Data-Trust Computation," International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2011, pp.51-58, 26-28 Oct. 2011.

[9] I.A. Sumra, H. Hasbullah, J.A. Manan, A.Iftikhar, "Trust levels in peer-to-peer (P2P) vehicular network," 11th International Conference on ITS Telecommunications (ITST), 2011, pp.708-714, 23-25 Aug. 2011.

[10] J. Blum, A. Eskandarian,"The Threat of Intelligent Collisions", IT Professional, IEEE Computer Society 2004.

©2012-13 International Journal of Information Technology and Electrical Engineering

AUTHOR PROFILES

Irshad Ahmed Sumra received his Bachelor Degree in Computer Science from Islamia University Bahawalpur in 2001. He pursued his MSC and MS in communication and network from Bahria University Islamabad, Pakistan in 2002 - 2007. Currently he is PhD student in Department of Computer and Information Sciences, Universiti Teknologi PETRONAS, Perak, Malaysia. His research interest includes Intelligent Transportation System (ITS)**,** security and Trust in Vehicular Ad hoc Networks (VANET).

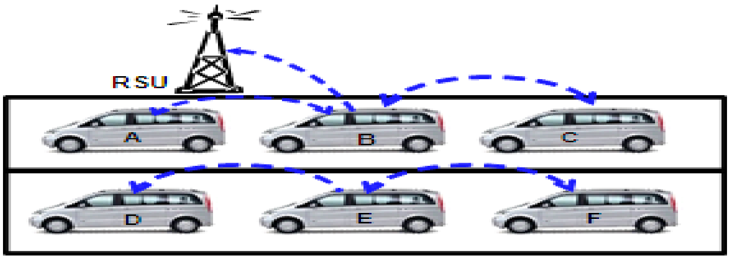
Assoc. Professor Halabi Bin Hasbullah received his Ph.D. degree in Electrical, Electronics and System Engineering from National University of Malaysia (Universiti Kebangsaan Malaysia), Malaysia in 2007. He is currently faculty member in the Department of Computer and Information Sciences at Universiti Teknologi PETRONAS. In the recent years, he has been involved in 4 research projects, inclusive VANET and VoIP. Dr. Halabi’s current research interests include wireless sensor networks, Bluetooth radio networks, ad hoc wireless networks, mobile computing, and VANET.

Jamalul-lail Ab Manan graduated from the University of Sheffield, UK with a Bachelor in Electrical Engineering (B.Eng). He pursued his Master of Science (MSc) in Microprocessor Engineering from University of Bradford, UK and PhD in Communications Engineering from University of Strathclyde, Glasgow, UK. He is currently a Senior Director at Advanced Information Security Cluster, MIMOS Berhad. He has 18 years of experience in teaching Electrical and Electronics, Microprocessor Engineering and Network Security. He has many years of industrial experience as Network Engineer, Senior Manager and Senior Vice President in ICT based government lined companies in Malaysia. In MIMOS Berhad, his current research focus is Information Security, particularly in Trusted Computing and Privacy Enhancing Technologies.

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

©2012-13 International Journal of Information Technology and Electrical Engineering



Definition: Trust (B, C, L2, B ↔ C, X (+))
Trust (B, R, L2, B ↔ R, X (+))

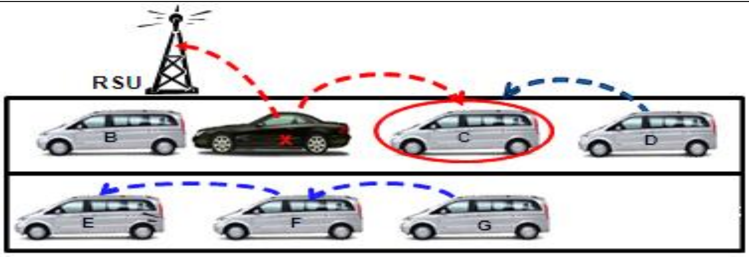
Find the Degree of Trust for Entity (B).

Entity (*e*B): B to C and B to RSU Communication are ok and sending and receiving is ok.

Trust Level (*l*): TL 2.

Action (a): Behaviour of all components is positive.

Strong Trust



Definition: Trust (C, D, L1, C ↔ D, X (+))
Trust (C, X, L0, X (-))

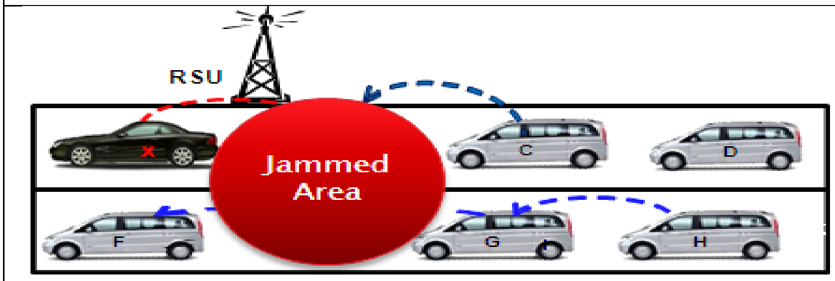
Find the Degree of Trust for Entity (C).

Entity (*ec*): C to D Communication is ok and C to X is not ok.

Trust Level (*l*): TL 1.

Action (a): Behaviour of some components is positive and negative in network.

Weak Trust



Definition: Trust (C, R, L0, X (-))
Trust (C, G, L0, X (-))

Find the Degree of Trust for Entity (C).

Entity (ec): C to RSU and entity G Communication is not ok due to attack.

Trust Level (*l*): TL 0.

Action (a): Behaviour of all components is negative due to Dos attack (channel jammed).

Zero Trust

Figure 14. Trust Levels with definitions