The Impact of Jamming on Threshold-Based Agreement in VANET

Hani Alturkostani
Department of Computer Science
University of Idaho
Moscow, Idaho 83843-1010
Email: altu2655@vandals.uidaho.edu

Axel Krings
Department of Computer Science
University of Idaho
Moscow, Idaho 83843-1010
Email: krings@uidaho.edu

Abstract*—In Intelligent Transportation Systems (ITS), Dedicated Short Range Communication (DSRC) enables communication among vehicles (V2V) and vehicles to infrastructure (V2I). ITS safety applications are designed to increase road safety and to reduce accidents. The reliability of DSRC-based ITS safety applications is essential. Thus, improving resiliency against faults, and enhancing reliability, are primary goals. Research has shown that threshold-based agreement methods effectively reduce the impact of value faults through validating events, by receiving the Basic Safety Message (BSM) from multiple sources. Whereas previous work considered value faults, e.g., injection, data fabrication and sensor manipulation, it does not address the impact of omission faults and jamming. This paper investigates the impact of jamming on threshold-based agreement in Vehicular Ad Hoc Networks (VANET). It is shown that jamming drastically reduces the correctness of the voted upon decision. We consider the Emergency Electronic Brake Lights (EEBL) safety application, and demonstrate how jammer position and power affect the correctness of the decision. Furthermore we show how the number of vehicles impacts the correctness of decisions in the presence of jamming. Finally a new adaptive threshold algorithm is introduced that improves the resilience against jamming attacks compared to algorithms presented in previous research.

I. Introduction and Background

Intelligent Transportation Systems (ITS) are expected to improve the driving experience and aim to reduce the number of road accidents. A core technology to accomplish this goal is wireless communications, specifically wireless vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. ITS provides a variety of useful applications, the most important of which are safety applications that will help prevent collisions and increase driver's awareness. It is estimated by the United States Department of Transportation (USDOT), that V2V communication based on DSRC can prevent up to 82% of all crashes in the United States involving unimpaired drivers, potentially saving thousands of lives and billions of dollars [1]. Safety applications rely on periodic Basic Safety Message (BSM) exchanges among vehicles and between vehicles and the infrastructure. The communication among vehicles and infrastructure require a solid underlaying platform that consists of well-defined technologies that ensure safe, stable and reliable system operation. V2V and V2I communication is based on Dedicated Short Range Communication (DSRC). A set of industry standards has been published to address proper interoperability, including [2], [3], [4], [5], [6], [7], [8]. Vehicles will be equipped with On Board Units (OBU) for inter-vehicular communication as well as communication with stationary Road Side Units (RSU). The Federal Communication Commission (FCC) has licensed the use of the 5.850-5.925 GHz (5.9 GHz band) for the DSRC services [9].

The focus of this research is on safety application reliability, which is of great concern, as the ITS is part of a critical infrastructure. The wireless communication at the core however inherits the full spectrum of potential vulnerabilities and attacks, and any failure may have catastrophic consequences, e.g., injury or loss of life. Furthermore, any compromise, may it be due to benign or malicious reasons, has the potential to undermine public trust and acceptance of these technologies. Conventional security measures, such as digital certificates, tamper-proof hardware and network security schemes are not sufficient [10]. Therefore it is paramount that mechanisms to increase reliability in the presence of faults are designed into the system, rather than in an add-on fashion. In order to increase reliability of DSRC safety applications such as crash avoidance or intersection collision applications, agreement has been suggested [10], [11] as a mechanism to tolerate faults.

In this paper we investigate threshold-based agreement algorithms under the effect of jamming. In particular, we study the impact of jamming on the Emergency Electronic Brake Lights (EEBL) application, and provide a new adaptive algorithm for accurate threshold calculation. First however some background information will be introduced.

A. Basic Safety Message

According to [3] the basic safety message (BSM) is used in a variety of DSRC safety applications to exchange safety data containing a vehicle's state. The BSM is broadcast at a transmission rate of 10 messages per second to surrounding vehicles. A BSM consists of two parts. The first part is required and contains data included in every BSM. The second part is optional and includes additional information for certain applications.

The required part of the BSM message contains the following: *DSRC_MessageID* is the first value in the BSM message and is used to define the message type, and to inform the receiving application how to interpret the remaining bytes.

MsgCount is used to sequence messages that were sent by the same sender with the same *DSRC_MessageID*. *TemporaryID* is used to identify the local vehicles that are interacting during an encounter. The value will periodically change to ensure the overall anonymity of the vehicle. *DSecond* provides current timing information, and is a simple value consisting of integer values representing the milliseconds within a minute. *Latitude* and *Longitude* provide the geographic latitude and longitude of an object, expressed in 1/10th integer micro degrees. *Elevation* represents the geographic position above or below the sea level. *PositionalAccuracy* consists of multiple parameters to represent the accuracy of the geographic position with respect to each axis. *TransmissionAndSpeed* expresses the current speed value in unsigned units of 0.02 meters per second combined with transmission state value. *Heading* provides the current heading and the orientation of the vehicle. *SteeringwheelAngel* expresses the rate of change of the angel of the steering wheel in either direction. *AccelerationSet4Way* provides acceleration values in 3 orthogonal directions, in addition to yaw rotation rates. *BrakeSystemStatus* provides information about current brake system status, (brake usage, anti-lock brake status, auxiliary brake status), in addition to system control activity of the vehicle. Lastly, *VehicleSize* indicates the vehicle length and width.

B. Jamming and Fault Types

Jamming, which is the fault source addressed in this research, is the act of emitting radio signals that interfere with the intended communications. Different jammer types have been introduced and characterized in [12], [13], ranging from constant jammers, which constantly disrupt communication brute force, to intelligent jammers that are protocol-aware and able to target specific data or control packets. Our initial focus is on constant jammers, which are considered the most disruptive as they indiscriminately affect all ongoing communication.

It should be noted that usual jamming mitigation techniques, such as those based on spread spectrum, are not applicable in DSRC, as the channels are fixed in their spectrum and the safety channel, which is Channel 172, is deticated to DSRC safety applications [2].

In general, we consider faults in the context of the fault model of [14]. A fault model is a taxonomy of fault types, and much research has addressed the redundancy levels needed to overcome specific fault types or mixes of fault types. Constant jamming, in the context of this research, has the potential to introducing *omissive symmetric* faults, which imply that a message is not received by any node. However, it also has the potential to cause *strictly omissive transitive* faults, where only a subset of nodes receive the message. It should be noted that we assume that jamming does not result in value faults, i.e., wrong messages, which would be considered *transmissive symmetric* faults under that fault model.

C. Safety Applications: Emergency Electronic Brake Lights

The DSRC safety application selected for demonstration in this paper is the Emergency Electronic Brake Lights (EEBL) application. According to [3] and [15], when a vehicle breaks hard, the EEBL safety application communicates this event to surrounding vehicles via one or more BSMs. The safety application helps drivers following the vehicle emitting the event by generating an early notification that the lead vehicle is braking hard. This is especially useful if the driver's visibility is impaired, e.g., due to low visibility as the result of poor weather conditions or a vehicle in line of site. Standard [3] further states that it is assumed that the vehicle braking hard is equipped with a DSRC unit and that the message from the vehicle is received by the following vehicles, specifically vehicles in relevant positions. The following describes the flow of events. Upon hard braking, the lead vehicle sends a BSM with additional information about the hard braking event, such as a hard-braking event flag, deceleration, and brake pressure. The following vehicles receive and process the message and infer that the message is relevant, i.e., it refers to a similar heading in advance of the lead vehicle's path, where a hard braking event is taking place. The receiving vehicle warns the driver about the braking event and its severity.

II. Related Work

Schemes based on voting and information validation in VANET have been presented in [10], [11], [16], [17], [18]. The most relevant to the work presented here will be discussed in more detail.

In [10] the authors proposed four static agreement methods, which are based on voting schemes that enforce plausibility checks to reach a correct decision in the presence of value fault. The decision methods are *Freshest Message*, which take into account the most recent messages received, *Majority Wins*, which performs local voting over all received messages regarding a certain hazard, *Majority of Freshest X*, which is a combination of the previous two methods considering the recent x messages, and *Majority of Freshest X with Threshold*, which is an extension of the previous method in addition to a threshold check. Their work did not specifically take into account the choice of the number of messages.

In [11] agreement is accomplished by making the application wait for a number of BSMs before warning the driver, based on the decision method "majority of freshest messages with threshold" introduced by [10]. However their focus was on dynamic determination of the threshold. Choosing the value of the number of messages was established by dynamically choosing the threshold according to current neighborhood density within transmission range R. The dynamic methods have been further divided into *dynamic naive*, which chooses a threshold based on the number of one-hop neighbors at time t, *dynamic naive ahead*, which chooses a threshold based on the number of one-hop neighbors at time t ahead of the current vehicle, and *majority ahead*, where the threshold is determined by taking half of the number of one-hop neighbors plus one at time t ahead of the current vehicle. However, their work did not take into consideration omission faults.

In [17] the authors proposed a voting algorithm using the participation of vehicles to prevent malicious data manipulation, fabrication or modifying the functioning of a vehicle's On Board Equipment to carry out attacks. They take into consideration certain abuse cases such as false speeding, false congestion, false braking, false timing and position data and higher message frequency. Voting is based on a predetermined confidence value.

The research in this paper considers the model of [10] and [11], which will be extended to consider the impact of jamming.

III. Agreement in VANET

In voting algorithms the selection of the correct threshold is essential. Selecting the threshold too low can increase the number of *false negatives*, i.e., the vote results in the faulty decision/value. Conversely, selecting the threshold too high results in high latency and exceeding safety time. The two methods for calculating the threshold have been discussed in the literature [10], [11] as static and dynamic thresholds. *Static* thresholds imply that the number of messages required for a decision is predetermined. The host vehicle waits for distinct number of messages regarding an event to be received. The decision to warn the driver or not is made by voting on what is being reported by the majority of vehicles. However, this method ignores variation in the neighborhood topology over time. As a result, the threshold might become insufficient in dense topologies, leading to premature decisions with high chance of false negatives. On the other hand, the threshold could become higher than required in sparse neighborhoods, which may also lead to undesired decision delay due to a lack of messages.

Dynamic threshold varies over time. Now the number of required messages is determined based on the number of vehicles in the surrounding neighborhood. However, the number of neighboring vehicles is taken without clear distinction of how the vehicles are positioned. This may lead to inaccurate threshold, because not all surrounding vehicles are witnessing the event. Even taking the number of vehicles ahead does not necessary grantee a correct threshold, because some ahead vehicles fall inside the transmission range, while being outside of the witnessing/detection area.

Jamming can impact the threshold selection. In the case of an event the subset of honest vehicles that detect the event will generate a true alert. However, due to jamming, one or more alerts may not be received by other vehicles. In fact, a malicious jammer may have a great advantage, e.g., by disrupting communication just after and event occurred. Furthermore this malicious event may have been coordinated with the jammer.

The general timing associated with threshold-based agreement is shown in Figure 1. The values associated with an event i, as they are extracted from BSM messages, are represented by the squares. These are the values received by the host vehicle running the DSRC safety application. Of special interest is the voting set, which contains the values received from the beginning of an event to the decision threshold. Again, the threshold is the number of message required before voting. This decision has to be made before time T_{safety}, which accounts for reaction and breaking time.

In a pathological attack the coordinating adversaries would attempt to maximally stack faulty values into the voting sets. Then, as values from other vehicles that contradict the fault event arrive, a correct vote can be made once the number of correct values exceed the number of faulty values. An example of such pathological scenario is shown in Figure 2, where 35 faulty values were stacked into the voting set at time $t = 0$. Then correct messages arrive until the time by which the threshold is achieved. In the example the threshold was set to 75, which was met at $t = 0.6s$, and the voting set contained 35 faulty and 40 correct values. In the example, the voting value is of course decided when the 36^{th} correct value arrives.

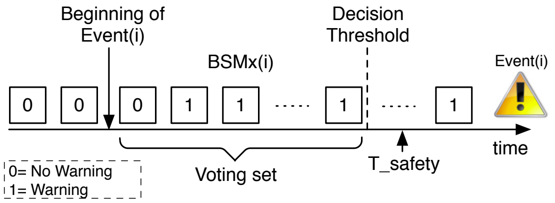

Fig. 1. Threshold-based agreement using voting in VANET

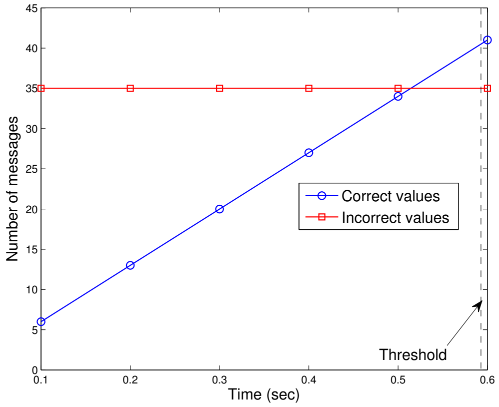

Fig. 2. Reaching correct decision as correct values outvote incorrect values

Now assume a pathological malicious case where the time of an event is coordinated with the jammer. Just after the event and stacking of the voting set with false values, the jammer starts impairing communications of correct values. The scenario of Figure 2 now deteriorates to the scenario shown in Figure 3. Here the threshold would be set lower, as fewer message arrive, wrongly suggesting lower vehicle density. Voting at time $t = 0.8s$ now results in a false negative.

IV. System Model

The overall model associated with threshold-based agreement in VANET is based on the areal model used in [11] and will be explained using Figure 4 showing a single lane of traffic. Following and event i, e.g., stopped vehicle or approaching game, two distinct areas are considered, i.e., the detection and decision area. In the detection area, denoted by $D_{detect}(i)$, the driver of each Remote Vehicle RV_j, $1 < j < n$,

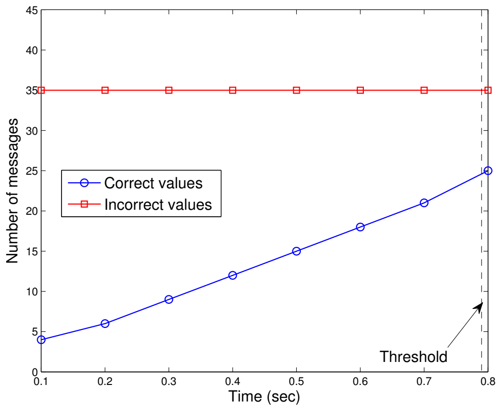

Fig. 3. Reaching incorrect decision as incorrect values outvote correct values with support from jammer

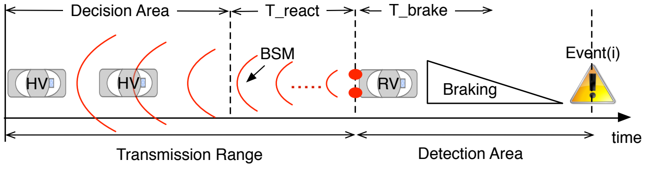

Fig. 4. System model for EEBL safety application

either has visual or autonomous sensing capabilities for detecting the hazard. The range of $D_{detect}(i)$ is bounded by the human vision and sensors capabilities, which in turn are subject to physiological and environmental conditions. In the decision area, denoted by $D_{decide}(i)$, each Host Vehicle HV_k, $1 < k < n'$, is distant from event i, but still within the transmission range R of RV_j. The group of vehicles RV_j located inside $D_{detect}(i)$ detect event i, e.g., the driver of the detecting vehicle brakes, thus triggering a $BSM_x(i)$ regarding event i, where x is a sequence number. $BSM_x(i)$ contains the information referred in Subsection I-A, such as location, speed, deceleration rate and brake intensity (brake flag). $BSM_x(i)$ will be received by host vehicles HV_k inside $D_{decide}(i)$, as long as it is within the transmission range R of RV_j. Thus, after receiving $BSM_x(i)$, vehicle HV_k infers a hazard as long as it is relevant to its current position.

When considering agreement, HV_k will accept BSM messages from different sources until a threshold of α has been received, or before reaching the maximum safety time for making a decision, which is the sum of reaction time T_{react} and required time for braking T_{brake}.

A. Attacker Model

The attacker is assumed to be a constant jammer. It is stationary on the side of the road, targeting any HV_k in area $D_{decide}(i)$, as can be seen in Figure 5, where it is positioned to maximize its effect. As HV_k approaches the jammer, the impact of jamming becomes more severe, thereby increasing the packet error probability P_p. The distance of HV_k to the jammer has great impact on P_p.

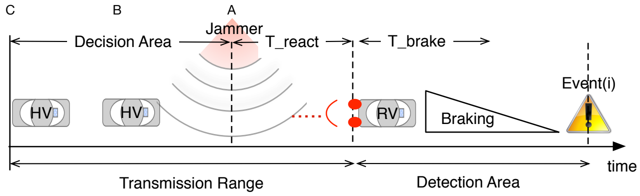

Fig. 5. Attacker model for EEBL safety application

Three different jammer positions have been examined in Figure 5. Positions A, B, and C are at the beginning, middle, and far-end of the decision area respectively. Our focus is on position A, as it gives the advantage to the jammer by being closer to HV_k at the time of event i. This increases P_p, thus decreasing the Packet Delivery Ratio at $D_{decide}(i)$ compared to the other two positions. The impact of the jamming power on the packet delivery ratio for the different positions is shown in Figure 6.

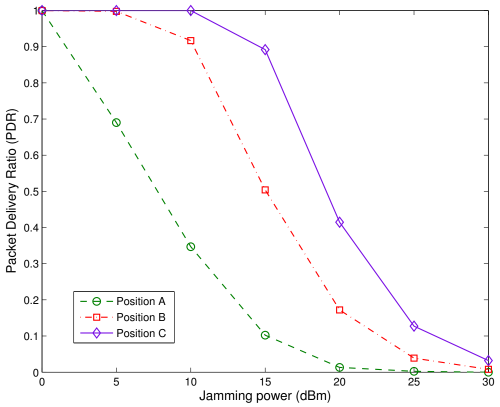

Fig. 6. The impact of jammer position on Packet Delivery Ratio in $D_{decide}(i)$

V. Adaptive Threshold Algorithm

We next present an adaptive threshold algorithm which has improved performance over those introduced in [10], [11]. The algorithm shown in Figure 7 allows HV_k to choose a threshold value $\alpha(t)$, defined below, based on the number of vehicles in the detection area $D_{detect}(i)$ at time t and before reaching T_{safety}. When HV_k receives a BSM message it first checks the location for relevance. If it is relevant to HV_k's current position and has not been recognized as a previous event, it checks the content for hazard inference, e.g., in the case of EEBL safety application it checks the brake flag. If a new hazard has been detected by HV_k, the algorithm initializes a new event location $i + 1$, calculates T_{safety} based on HV's current speed and location, and further increases the RV count by one. The algorithm also proceeds with incrementing the warning counter and the total count of received BSM regarding the event by one, and the current time is checked against

T_{safety}. If T_{safety} has been reached, a prompt decision must be made. Otherwise it checks whether it has received enough BSM messages to reach threshold $\alpha(t)$. If the check is true it initiates voting and makes a decision. The process is repeated in case there is still time to T_{safety} or the threshold has not yet met. Threshold $\alpha(t)$ is determined at time t based on the number of vehicles in $D_{detect}(i)$ by

$$\alpha(t) = P(\lambda) \times N(D_{detect(i)}(t)) \tag{1}$$

where $P(\lambda)$ is a percentage of the recent BSM arrival rate λ, and $N(D_{detect(i)}(t))$ is the number of vehicles in the detection area for event i at time t.

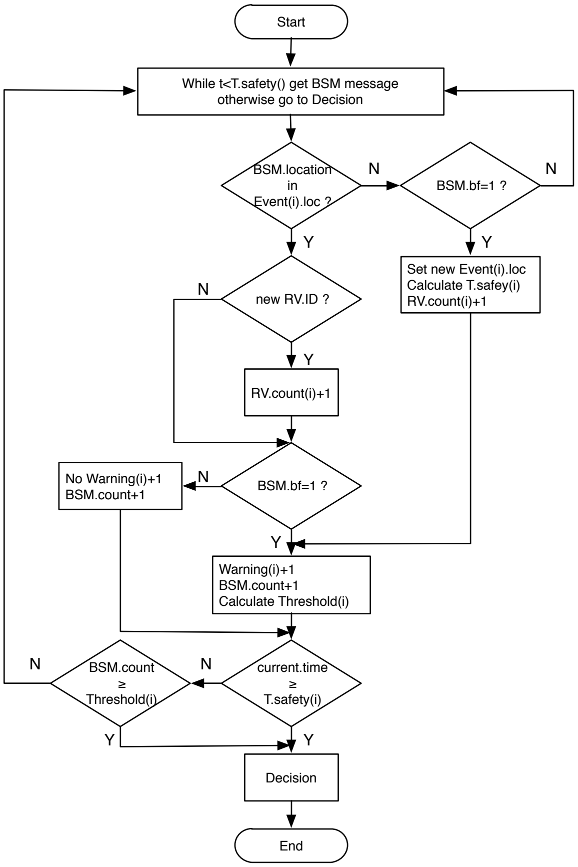

Fig. 7. Adaptive threshold algorithm

VI. Performance Evaluation

The performance of the new adaptive threshold algorithm was compared against the algorithms in [10], [11] using a two-stage model, i.e., the "car following mobility model" of [19] as input to Matlab, which calculated the false negative rates based on the jamming and communication model of [20]. The evaluation was for the EEBL application in a single lane road attacked by a jammer with specifications equal to an OBU. Further assumptions were that BSM messages cannot be forged and that transmission errors due to collations are negligible due to the overall low traffic density. The simulation parameters were set according to Table I.

Simulation software	Matlab
Simulation duration	120 *sec*
Transmission range	300 *m*
Number of vehicles	5-55 vehicle/*km*
Vehicle speed	15 *m/sec*
Reaction time	1 *sec*
BSM generation	every 100 *msec*
Bandwidth	8.3 MHz
Data rate	6 Mbps
Transmitter power	20 dBm
Jammer power	5-30 dBm

TABLE I
Simulation Parameters

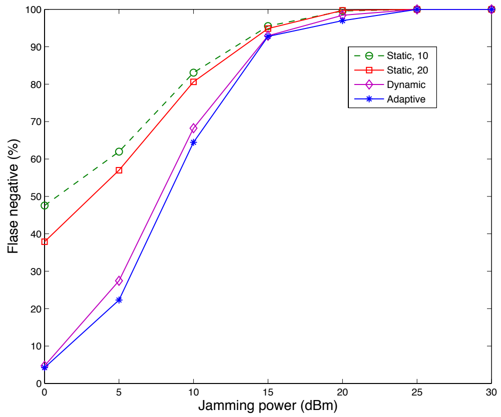

Fig. 8. The effect of jamming power on threshold algorithms

Figure 8 shows the effect of jamming on the decision making process for the new adaptive threshold algorithm, the static threshold algorithm of [10] with thresholds 10 and 20, and the dynamic algorithm of [11]. Jamming power ranged from 5 dBm to 30 dBm; 0 dBm represents the case without jamming. The traffic density was fixed at 45 vehicles/km. It can be seen that all algorithms are very sensitive to the impact of jamming. However, the dynamic and the adaptive algorithms show the highest resistance against this impact, with modest advantage of up to 5% to the adaptive algorithm.

One may ask the question about the usefulness of the algorithms if they are so affected by jamming. The answer however is that if the impact of jamming is high, jamming detection can be used to steer the application to a fail-safe mode. That is, if jamming is detected the application can alert the driver about the unavailability of the application. It is the lower powered jamming that is harder to detect, and that is the range in which the algorithms are most useful. The false negative rates at 0 dBm are due to vehicles in the decision area, specially those at the back end, that fall outside of the transmission range of some vehicles at the very front of the detection area. However, vehicles at the backend of the decision area would still receive alert messages, but not enough to reach the static threshold, hence resulting in high false negative. Figure 9 shows the effect of vehicle density on different threshold algorithms with jamming power fixed to 10 dBm. When traffic is sparse the chances of making faulty decisions is the highest. This is due to larger inter-vehicle spacing, and thus vehicles in the decision area are more affected by jamming. This is because of the jammer's proximity to the host vehicle in comparison to other remote vehicles in the detection area. The result is that the number of messages being received by the host vehicle is insufficient, which in consequence results in higher false negative rates. As the traffic becomes more dense, the decisions improve even in the presence of moderate jamming. The adaptive algorithm performs modestly better in all situations, i.e., up to 4%. As in the discussion of the previous figure, the high false negative rate in the presence of jamming highlights the need for jammer detection. It should be noted that the false negative rate at a vehicle density of 45 vehicles/km also appears in Figure 8 for 10 dBm jamming power.

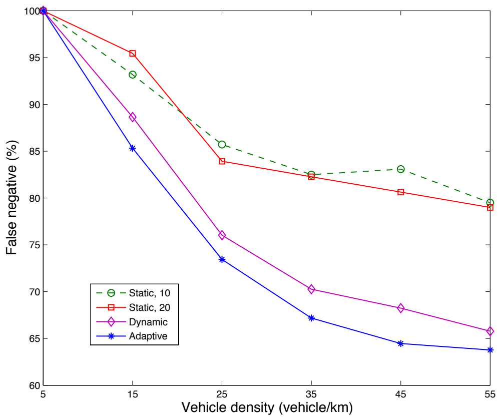

Fig. 9. The effect of vehicle densities on agreement algorithms

VII. Conclusion

DSRC safety application reliability was investigated in Intelligent Transportation Systems subject to benign and malicious faults. Since the ITS is part of a critical infrastructure, application reliability is essential. In order to minimize faulty decisions made by DSRC safety applications about events, e.g., detection of – and reaction to hazards, agreement has been found to improve detection of fault event notification, such as warnings or revocation thereof. This paper investigated the impact of jamming on threshold-based agreement algorithms, such as static, dynamic, and adaptive algorithms. It was shown that constant jamming can drastically decrease the decision quality for these threshold-based agreement algorithms. A new adaptive threshold algorithm was also presented that provides higher resilience against jamming. The performance of the new adaptive threshold algorithm and its resilience against jamming were investigated using the Electronic Emergency Brake Lights safety application defined in the VSC-A project and J2735 standard. The new algorithm was shown to outperform its counterpart, due to the nature of adaptively adjusting the voting thresholds. Whereas the observed improvements were by modest 2-5%, these improvement should be seen in the context of saving lives. While threshold-based agreement algorithms in VANETs are effective in the presence of faulty nodes or low power jamming, they deteriorate as the jamming power increases. Specifically, the observations of the false negative rates when the EEBL application was subjected to jamming with higher power levels suggest the need for jamming detection in order to transition the application to a fail-safe state.

References

[1] J. B. Kenney, *Dedicated short-range communications (dsrc) standards in the united states*, Proceedings of the IEEE, vol. 99, no. 7, pp. 1162 1182, 2011.

[2] *Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems - 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, ASTM E2213-03, 2010.

[3] *Dedicated Short Range Communications (DSRC) Message Set Dictionary. Society of Automotive Engineers*, SAE J2735, November 2009.

[4] *IEEE Standard for Information technology–Telecommunications and information exchange between systems–Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments*, IEEE Std 802.11p, 2010.

[5] *IEEE Draft Guide for Wireless Access in Vehicular Environments (WAVE) -Architecture*, IEEE P1609.0/D5, September 2012.

[6] *IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages*, IEEE Std 1609.2TM, 2013.

[7] *IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services*, IEEE Std 1609.3TM, 2010.

[8] *IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operation*, IEEE Std 1609.4TM, 2010.

[9] *Amendment of the Commission's Rules Regarding Dedicated Short-Range Communication Services in the 5.850-5.925 GHz Band (5.9 GHz Band)*, Federal Communications Commission FCC 03-324, 2004.

[10] B. Ostermaier, F. Dotzer, and M.Strassberger, *Enhancing the security of local danger warnings in vanets - a simulative analysis of voting schemes*, in Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on. IEEE, 2007, pp. 422431.

[11] J. Petit and Z. Mammeri, *Dynamic consensus for secured vehicular ad hoc networks*, in Wireless and Mobile Computing, Networking and Communications (WiMob), 2011 IEEE 7th International Conference on. IEEE, 2011, pp. 18.

[12] K. Pelechrinis, M. Iliofotou and S. V. Krishnamurthy, *Denial of Service Attacks in Wireless Networks: The Case of Jammers*, Communications Surveys & Tutorials, IEEE , vol.13, no.2, pp.245,257, 2^{nd} Quarter 2011.

[13] W. Xu, W. Trappe, Y. Zhang and T. Wood, *The feasibility of launching and detecting jamming attacks in wireless networks*, In Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, pp. 46-57. ACM, 2005.

[14] M. H. Azadmanesh and R. M. Kieckhafer, *Exploiting omissive faults in synchronous approximate agreement*, Computers, IEEE Transactions on, vol.49, no.10, pp.1031,1042, Oct 2000.

[15] Vehical Safety Communications-Applications (VSC-A) Final Report. DOT HS 811 492 A. U.S. Department of Transportation, NHTSA. September 2011.

[16] Z. Cao, J. Kong, U. Lee, M. Gerla, and Z. Chen, *Proof-of-relevance: Filtering false data via authentic consensus in vehicle ad-hoc networks*, in INFOCOM Workshops 2008, IEEE. IEEE, 2008, pp. 16.

[17] G. Di Crescenzo,Y. Ling, S. Pietrowicz, and T. Zhang, *Non-interactive malicious behavior detection in vehicular networks*, in Vehicular Networking Conference (VNC), 2010 IEEE. IEEE, 2010, pp. 278285.

[18] M. Raya, A. Aziz, and J.-P. Hubaux, *Efficient secure aggregation in vanets*, in Proceedings of the 3rd international workshop on Vehicular ad hoc networks. ACM, 2006, pp. 6775.

[19] A. D. May, *Traffic Flow Fundamentals*, Englewood Cliffs, NJ: Prentice-Hall, 1990.

[20] A. Serageldin, and A. Krings, *The Impact of Redundancy on DSRC Safety Application Reliability under Different Data Rates*, Proc. 6th International Conference on New Technologies, Mobility and Security, (NTMS 2014), Dubai, March 30 - April 2, 2014.