Relevance-based Verification of VANET Safety Messages

Subir Biswas
Department of Computer Science
University of Manitoba
Winnipeg, Canada R3T 2N2
Email: bigstan@cs.umanitoba.ca

Jelena Mišić
Department of Computer Science
Ryerson University
Toronto ON, Canada M5B 2K3
Email: jmisic@scs.ryerson.ca

***Abstract*—Authentication of vehicular safety messages poses a challenge in a high density road-traffic scenario as the verification time for gathered messages gets longer than the average inter-arrival time. This may expose a vehicular network entity to several different security attacks. The existing solutions have addressed the issue either by randomizing the verification candidates, or by using aggregated signature verification schemes, both of which have short-comings in terms of applicability in vehicular communications. We propose a novel solution to the vehicular message authentication in dense traffic conditions by introducing a prioritized verification strategy. Based on the relevance of physical parameters of neighboring vehicles, received safety messages are assigned with different priority scores at the verifying entity. In a heavy traffic condition when the resources are scarce, a verifier randomly authenticates the selected received messages according to their priorities. Performance evaluation has shown that our approach is scalable, resource-efficient, and compatible with any underlying authentication schemes.**

I. Introduction and Motivation

With the goal of enhancing driving safety in roads and highways, a Vehicular Ad hoc Network (VANET) enables its users to exchange traffic and other application-oriented messages. An On-board Unit (OBU)- installed with a vehicle may periodically broadcast the vehicle's current position, acceleration/deceleration, and speed information to the neighboring entities. Authentication of such information is crucial since a user may need to take an important safety measure based on the compiled messages from the neighboring entities.

Unfortunately, verification of authenticity incurs a cryptographic processing delay at the receiving end. It may look negligible for an individual task, although in a high density traffic scene with hundreds of vehicles in the communication range, a node would essentially receive an enormous load of messages per unit time, causing a bottleneck at the authentication process.

Therefore, road-safety applications under a dense traffic scenario are either to be performed with a high risk of several different malicious attacks on VANET, or to be constrained by a random portion of messages which got verified. In either case, the ultimate target of having enhanced driving safety on road is not achieved.

Related literature has addressed the problem of authenticating several signed messages per unit time in two major ways- random verification of signed messages, and aggregated (batch) verification of all the received messages.

In a random verification of signatures, received messages are randomly picked for verification by a receiving entity. The idea has been incorporated for VANET by Raya et al. [1] to obtain scalability in signature verification process. Guo et al. [2] used random verification for a group signature-based anonymous authentication in VANETs where it is claimed that about 95% of the total received messages are verified if each OBU randomly picks three messages on an average for verification. Several other VANET authentication schemes (e.g. [3], [4]) adopted this technique for its network scalability and simplicity. The success of a random verification approach is highly reliant on traffic density, or the number of participants in the VANET, and therefore, un-sustaining.

On the other hand, a batch verification technique in VANET is used for authenticating all received messages at a time. However, this mechanism is completely dependent on the underlying signature scheme used in VANET. A batch verification can not isolate an individual signature failure, and rejects all received messages irrespective of the authenticity of other valid messages. Cheon et al. [5] have proposed a fast batch verification using a bilinear pairing based authentication scheme. Bilinear pairing-based cryptographic approaches have been criticized in [6] as inefficient for practical implementation. Also, temporary storage for the verification of received messages imposes an extra requirement on VANET entities.

A resource-aware verification scheme for VANET messages has been presented by Li et al. [7] where received messages are verified based on the physical distance of the source. The received messages from the closest proximity of the receiver would be immediately authenticated, while rest of the messages are verified in a random fashion within the resource budget. In a sparse traffic scenario, this approach basically reduces to a simple random verification scheme as there is no vehicle in the proximity.

Our Relevance-based Verification scheme is an improvement of Li et al.'s scheme. Instead of considering the physical distance as the only relevance parameter, we propose an approach of message verification where priority of a received message is assessed based on the relevance of the safety information provided by the message.

We use a set of Bloom filters [8] to determine the relevance of received messages. A binary decision tree is constructed in order to categorize the received messages into different priorities based on their relevance. Received messages from different priority sets get a fair chance to be authenticated even in a very dense traffic condition.

In this approach, all the received messages would be verified as long as the total number of vehicles in the neighborhood surpass a maximum value. The size of the maximum value is specific to the signature scheme used in the VANET since different schemes require different amount of verification time. However, If the number of neighboring OBUs goes beyond the maximum value, received messages in an OBU are verified following a weighted probability scheme with respect to the physical characteristics of the network.

The rest of the paper is organized as follows. A brief discussion on WAVE security standards, ECDSA Signature, and Bloom filters have been provided in Section II. Section III describes our proposed idea of verification on relevance-based priority. Section IV provides the performance evaluation of related issues as the concluding remarks are posted in Section V.

II. Preliminaries

A. WAVE Security and ECDSA

An operating OBU periodically broadcasts beacons with its information on position, acceleration/deceleration, direction, and speed to its neighboring entities in the communication range [9]. The most typical beacon interval for safety messages ranges from 100 ms to 300 ms. The security services also adopt Elliptic Curve Digital Signature Algorithm (ECDSA [10]) for source authentication and message integrity in VANETs.

An implementation of ECDSA with P-224 curve [11] requires approximately 5 ms as indicated in [12], meaning that an OBU can verify maximum 200 messages per sec. Therefore, with a conventional one-by-one ECDSA verification, a receiving OBU would not be able to verify messages from more than 20 vehicles in the neighborhood assuming each VANET entity delivers signed messages at an interval of 100 ms.

B. Bloom Filters

A Bloom Filter [8] is a special type of data structure that contains a set $A = \{a_1, a_2, ..., a_n\}$ of n elements in order to answer the queries about the availability of any element $a \in A$. A Bloom Filter is represented by an array of M bits, all set to 0 at the initialization. The length of the bit array, M is termed as the *size* of the Bloom Filter. For the insertion of an element a into the Bloom Filter, the element a_i is individually processed by cryptographically secure k independent hash functions, $h_1(), h_2(), ..., h_k()$. The hash outcomes, $h_1(a), h_2(a), ..., h_k(a)$ are used as the indices of the array where the corresponding bits are set to 1. Figure 1 shows an insertion operation of an element a in a Bloom Filter.

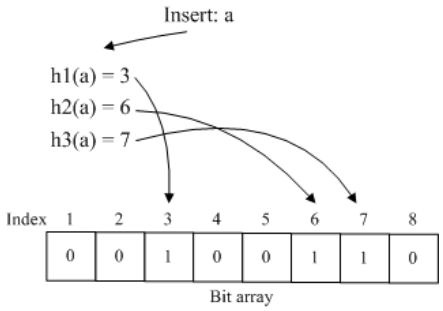

Fig. 1. A Bloom Filter with $k = 3$.

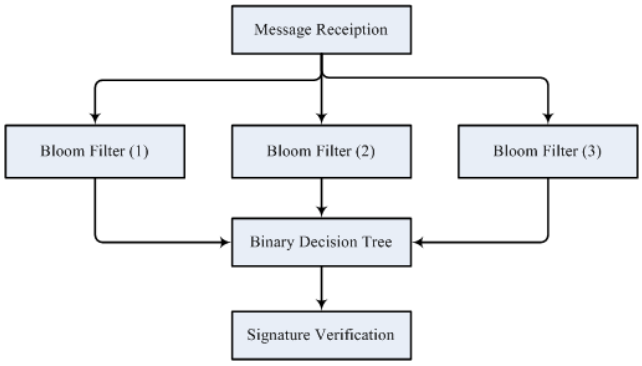

Fig. 2. Block diagram of our scheme.

When there is a query about the availability of particular element, the Bloom Filter uses the same set of k hash functions, and checks if all the hash outputs indicate 1s in the bit array. If any of those indexes set to 0, the element is certainly not present in the Bloom Filter. On the other hand, if all k hash results indicate 1s in the bit array, we consider that the element is present in the filter with error probability, P. The possibility of an error exists due to the potential cryptographic weakness of used hash functions. In fact, a practical implementation only uses one hash function for Bloom Filter applications, while different portions of the hash outcome are associated with k hash results [13].

III. Relevance-based Verification of VANET Safety Messages

A. The Framework

A general framework of our scheme is given in Figure 2. We consider the three most important physical traffic safety parameters for our relevance-based prioritized message authentication. Three different pieces of information are prioritized in the following order- current position of the sender OBU, acceleration/deceleration, and current speed of the vehicle. Three separate Bloom Filters are deployed in each verifier entity in order to update the most recent traffic scenario of the neighborhood. Each Bloom Filter individually checks the assigned portion of received information against the existing entries in the corresponding records within the bit array.

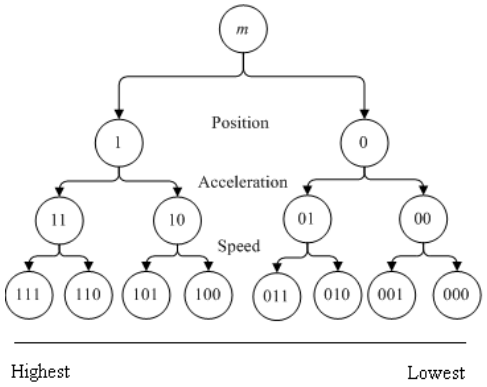

Fig. 3. The designed binary tree for relevance priority.

A perfect binary decision tree [14] as given in Figure 3 represents the mapping of the received messages with one of the priority sets based on the ordered relevance of the associated safety information of the message.

The root of the tree represents a received message *m*, while the other subsequent parent nodes indicate the responses from the associated Bloom Filters at each level. Every tree level corresponds to an individual safety parameter in the decreasing order of their priorities.

Up on reception, a periodic safety message's data payload is passed to the three designated Bloom Filters where each filter works on the specific part of the safety information with one of the three criteria mentioned above.

If a newly received message component *with an acceptable tolerance* matches with an existing entry in the corresponding Bloom Filter, it returns a 1. Otherwise, the Bloom Filter simply inserts the new entry in the assigned bit array, and returns a 0.

As indicated in Figure 3, on each level of the tree, a left child of a parent node represents the corresponding relevance of safety information, and assigned with a 1. On the other hand, a right child of a parent node on each level indicates the non-relevance of an associated safety parameter, and assigned with a 0. Assigned binary values from the parent nodes are joined together to represent the priority score of the subsequent children nodes of the decision tree. Each received message in a receiving VANET entity is associated with one of the priority scores defined by the leaves of the decision tree.

Our designed binary decision tree has eight leaves with the left most leaf containing the maximum relevance score. Messages belonging to this leaf are tagged with the highest priority of 7. As we move along from left to right at the bottom of the tree, the associated relevance as well as the priority of a corresponding message continue to get lower.

Let us assume that a receiving VANET entity can verify all the messages from at most v_τ vehicles per unit time. The small area in the neighboring proximity of the verifying entity, where maximum v_τ vehicles can be accommodated under the worst traffic condition is defined as the *safety zone* for that particular verifier.

We consider all received messages in a receiving OBU for a given duration (say, 1 sec). Received messages with priority tags are sequentially organized into some fixed size sets according to the decreasing order of message priorities. The size of a message set is determined by the maximum number of messages that can be verified per unit time by the underlying signature and verification scheme. If the total number of received safety messages in a receiver exceeds its verification capacity, selected received messages from across the priority sets would be verified.

Received messages from different priority sets are randomly verified with specific verification probability (pr_i) following a truncated geometric distribution as indicated in eqn. 1. Since vehicles in a close proximity have similar safety features in their periodic broadcasts, verification of a portion of a particular set of received messages would give a fair idea about the traffic safety condition in a dense traffic scenario.

$$pr_i = \frac{p^{(k-1)} \times (1-p)}{\sum_{i=1}^{N} p^{(i-1)} \times (1-p)}; \tag{1}$$

where pr_i is the verification probability of a received message, k is the priority set index, and p is the probability of an event.

We consider the event of packet loss in the communication channel as the foundation of the truncated geometric distribution to determine the weighted verification probability for the priority sets. Packet drop rate in a communication channel is proportional to the total offered load in the network. Since OBUs broadcast periodic safety messages of approximately same size, data packet drops in a VANET mainly due to the excessive OBUs in the communication range. Therefore, it would be rational for us to use the packet drop probability as the basis of determining the weighted verification probability for different priority sets of received messages.

IV. Performance Evaluation

We analyze the following performance issues of the proposed scheme.

A. Resiliency to Attacks

An adversary in a VANET scenario may try to launch a denial of service (DoS) attack by posting a huge number of unwanted messages to occupy the physical resources required for the authentication in one or more legitimate entities. Similarly, there can be a signature forging, or even a false message (e.g. lying about current position) attack by a malicious entity who wants to jeopardize the safe driving environment in a VANET.

Our approach allows relevance based probabilistic authentication according to the priority of received messages, where messages from the nearest proximity of an entity get higher priority than others. Therefore, messages from distant OBUs are less likely to be chosen for the verification. Since a high priority message is from the verifier's safety zone, either of these above attackers would be spotted easily by the verifying entity. However, in a sparse traffic scenario, all received

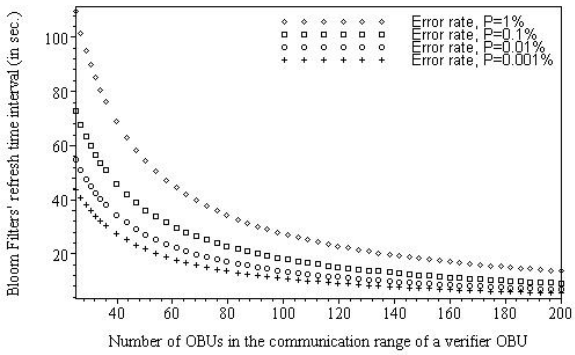

Fig. 4. The refresh interval of a Bloom Filter used in the proposed scheme.

messages belong to only a small number of priority sets of the verifier and hence they get verified with a greater probability.

B. Stabilizing the Bloom Filters

Frequent updates from the neighboring vehicles would contribute to the rapid growth of the number of elements in a Bloom Filter's bit array, affecting the performance of the filter with false positive errors as the size of a Bloom Filter is constant. A large size Bloom Filter may resolve the problem to some extent, but it aggravates the false positive rate for some of the elements in the bit array [15].

A *stable* Bloom Filter [16] stores only the most recent elements in the bit array with the requirement of extra spaces to save the history for each element of the bit array. Since there is no way to separate the most recent elements from the old ones in an ordinary Bloom Filter, we must clear the *aged* Bloom Filter, and re-load it with fresh elements at a regular interval in order to restrict the error probability up to a fixed value.

In a traffic scenario of N vehicles in the communication range of a verifier entity, let us assume that the refresh interval of a Bloom Filter is r seconds, and the periodic safety message delivery rate is f per second. Then, elements inserted into each Bloom Filter before resetting is computed as, $n = N \times r \times f$.

The relationship between the total number of elements n, and the Bloom Filter size M for an optimal use with a predefined error probability of P is given as, $n \approx M \times \frac{(ln2)^2}{|lnP|}$; [15].

Combining these two above relationships, we get:

$$r \approx \frac{M}{N \times f} \times \frac{(ln2)^2}{|lnP|}. \quad (2)$$

Figure 4 represents the required refresh interval of a Bloom Filter in our approach with different options of P. Values of the derived interval drop exponentially as the number of OBUs in the neighborhood increases. Depending on the road-safety design specifications and traffic plan, a specific curve can be chosen in order to optimize the operation of our scheme.

C. Simulation Setup

We evaluate our scheme using network simulator (ns-2.34) over DSRC IEEE 802.11p control channel (CCH). The simulation program is designed to work with the four EDCA categories [17] to provide different access priorities, from which we use the background traffic class (AC1) for periodic safety message broadcasts. Other access classes also provide quite similar results for periodic broadcasts of safety messages. Related PHY and MAC parameters are chosen from [5], [18], and summarized in Table I. Signed WSMP messages with 254 bytes payload have been considered for periodic safety messages following the IEEE 1609.2 standard [9].

TABLE I
SIMULATION PARAMETERS FOR MAC AND PHY

Parameters	Values
Simulation Area	$500 \times 100\ m^2$
Data Rate	3Mbps
CWMin	15
CWMax	511
Slot Time	16μs
SIFS	32μs
AIFS	144μs (9 slots)
Bandwidth	10MHz
Frequency	5.89GHz
Propagation Model	TwoRayGround

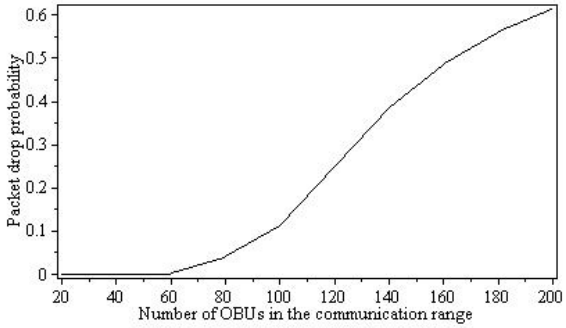

Fig. 5. Average packet drop rate per node.

We assume a simple urban vehicular traffic scenario in a 500 m long bidirectional road with 4 lanes in each direction. Individual vehicle's speed varies following a Gausian distribution with mean of 100 km/hr and standard deviation of 5 km/hr. For the packet drop due to the network congestion, we let each OBU to broadcast a WSMP packet every 100 ms. Times of message broadcast have been uniformly distributed over 100 ms period.

D. On Packet Loss and Verification Probability

Packet delivery in a wireless network is impaired due to the excessive offered load, and inherent noise of the medium. Figure 5 presents the packet drop probability of a DSRC control channel (CCH) used for vehicular communications. The probability of packet drop for an OBU hikes as the number of neighboring OBUs increases.

We use the packet drop probability as the basis of the probabilistic verification of received messages. For different number of vehicles in the communication range of an OBU, verification probability of messages from a particular prioritized set would be determined following the eqn. 1. The weighted verification probability of received messages in

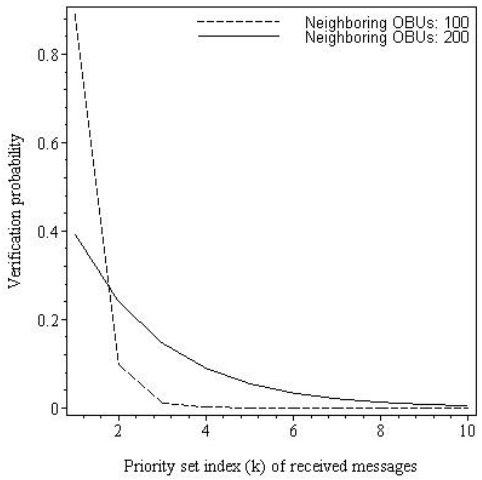

Fig. 6. Verification probability for prioritized sets of received messages.

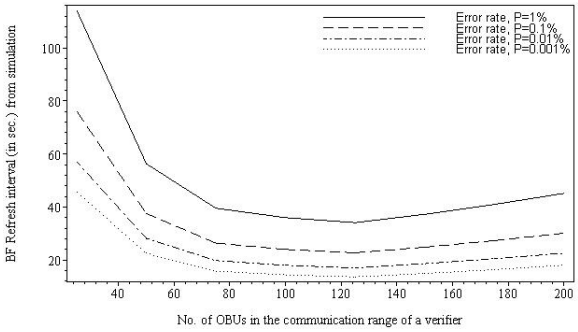

Fig. 7. The Bloom Filter refresh time interval obtained from the network simulation.

different priority sets is presented in Figure 6. As the number of total priority sets increases for the higher index value of the priority sets, the verification probability experiences an exponential decrease. However, the cumulative probability of message verification for all the priority sets is always 1.

The refresh rate of a Bloom Filter is also affected by the packet loss in the medium. Figure 7 plots the refresh interval of a Bloom Filter with packet loss for different number of OBUs in the communication range.

V. Conclusion

We introduced a new authentication strategy for VANET's safety message verification process. OBUs in a vehicular network periodically broadcasts safety messages containing road-safety information. Received messages in a VANET entity are first assigned with priority scores based on their relevance with the contemporary safety information of the receiver OBU. Prioritized messages are then divided into some fixed size priority sets. Messages from different priority sets get a fair share of verification resources. A truncated geometric distribution using the channel's packet loss probability for different number of OBUs determines the weighted probability of the verification of messages from a particular priority set.

Our scheme ensures the fairness with random verification, and it is compatible with any underlying signature and verification scheme, as well as the security standards for vehicular communications. Performance evaluation with security analysis and simulation results justify the scheme as an effective approach toward the growing prospects of vehicular ad hoc networks.

References

[1] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications," *Wireless Communications, IEEE*, vol. 13, no. 5, pp. 8–15, October 2006.

[2] J. Guo, J. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," May 2007, pp. 103–108.

[3] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "An efficient message authentication scheme for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 57, pp. 3357–3368, 2008.

[4] S. Biswas and J. Misic, "Location-based anonymous authentication for vehicular communications," in *PIMRC 2011: Proceedings of the 22nd IEEE Symposium on Personal, Indoor, Mobile and Radio Communications*. IEEE Communication Society, 2011, pp. 1–5.

[5] Q. Chen, F. Schmidt-Eisenlohr, D. Jiang, M. Torrent-Moreno, L. Delgrossi, and H. Hartenstein, "Overhaul of IEEE 802.11 modeling and simulation in ns-2," in *Proceedings of the 10th ACM Symposium on Modeling, analysis, and simulation of wireless and mobile systems*, ser. MSWiM '07. New York, NY, USA: ACM, 2007, pp. 159–168. [Online]. Available: http://doi.acm.org/10.1145/1298126.1298155

[6] S. D. Galbraith, K. G. Paterson, and N. P. Smart, "Pairings for cryptographers," *Discrete Appl. Math.*, vol. 156, pp. 3113–3121, September 2008. [Online]. Available: http://portal.acm.org/citation.cfm?id=1450345.1450543

[7] Z. Li and C. Chigan, "On resource-aware message verification in vanets," in *Proceedings of IEEE International Conference on Communications, ICC 2010, Cape Town, South Africa, 23-27 May 2010*. IEEE, 2010, pp. 1–6.

[8] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," *Commun. ACM*, vol. 13, pp. 422–426, July 1970. [Online]. Available: http://doi.acm.org/10.1145/362686.362692

[9] "IEEE trial-use standard for wireless access in vehicular environments (WAVE)- security services for applications and management messages," IEEE, New York, NY, IEEE Std 1609.2, Jul. 2006.

[10] D. Johnson and A. Menezes, "The elliptic curve digital signature algorithm (ECDSA)," Certicom Research, Canada; and Dept. of Combinatorics and Optimization, University of Waterloo, Canada, Tech. Rep., 1999.

[11] NIST, "NIST: national institute of standards and technology," http://www.nist.gov/index.html, 2011.

[12] J. Petit, "Analysis of ecdsa authentication processing in vanets," in *Proceedings of the 3rd international conference on New technologies, mobility and security*, ser. NTMS'09. Piscataway, NJ, USA: IEEE Press, 2009, pp. 388–392. [Online]. Available: http://dl.acm.org/citation.cfm?id=1790343.1790418

[13] F. Chang, F. Chang, and W. chang Feng, "Approximate caches for packet classification," in *In IEEE INFOCOM*, 2004, pp. 2196–2207.

[14] NIST, "NIST: national institute of standards and technology," http://xlinux.nist.gov/dads/HTML/perfectBinaryTree.html, 2011.

[15] P. S. Almeida, C. Baquero, N. Preguiça, and D. Hutchison, "Scalable bloom filters," *Inf. Process. Lett.*, vol. 101, pp. 255–261, March 2007. [Online]. Available: http://dl.acm.org/citation.cfm?id=1224252.1224501

[16] F. Deng and D. Rafiei, "Approximately detecting duplicates for streaming data using stable bloom filters," in *Proceedings of the 2006 ACM SIGMOD international conference on Management of data*, ser. SIGMOD '06. New York, NY, USA: ACM, 2006, pp. 25–36. [Online]. Available: http://doi.acm.org/10.1145/1142473.1142477

[17] "Draft amendment for wireless access in vehicular environments (WAVE)," IEEE, New York, NY, IEEE Draft 802.11p, Jul. 2007.

[18] J. Misic, G. Badawy, S. Rashwand, and V. B. Misic, "Tradeoff issues for CCH/SCH duty cycle for IEEE 802.11p single channel devices," in *Proceedings of the IEEE GLOBECOM 2010: Global Communications Conference*, 2010.