DoS attack-tolerant TESLA-based broadcast authentication protocol in Internet of Things

Na Ruan, Yoshiaki Hori
Department of Informatics, Kyushu University, Fukuoka, Japan
Email: ruanna@itslab.inf.kyushu-u.ac.jp, hori@inf.kyushu-u.ac.jp

***Abstract*—The Internet of Things (IoTs) is an emerging concept referring to networked everyday objects that interconnect to each other via wireless sensors attached to them. TESLA is a source authentication protocol for the broadcast network. Scalability of TESLA is limited by distribution of its unicast-based initial parameter. Low energy consumption version of TESLA is μTESLA, which is designed for wireless sensor network (WSN), while cannot tolerate DoS attack. TESLA++ is the DoS-tolerant version and is designed for VANET. TESLA++ cannot be accepted by WSN because of its higher consumption of power. To realize secure and robust DoS attack in the hybrid-vehicle-sensor network, we provide a TESLA-based protocol against DoS attack with a lower consumption of power. Analysis results demonstrate that using our protocol is better than using μTESLA or TELSA++, respectively.**

***Index Terms*—TESLA, Source authentication protocol, Broadcast communication, Hybrid-vehicle-sensor network, IoTs.**

I. Introduction

A. Background

Internet of things (IoTs) refers to uniquely identifiable objects (things) and their virtual representations in an Internet-like structure [1], [2]. Technologies like RFID, short-range wireless communications, real-time localization and sensor networks are now becoming increasingly common, bringing the Internet of Things into commercial use.

There is a wide range of networks (WSNs, VANETs, RFID, Smartphone, and others.), which are involved in building the IoTs. Because of such kind vast range of applications, elements in IoTs communicate via broadcasting messages, which make the messages' dissemination efficient. Correspondingly, securing broadcast communication protocol is brought into research.

TESLA (Timed Efficient Stream Loss-tolerant Authentication) [3] is lightweight securing broadcast communication protocol for source authentication. It uses purely symmetric cryptographic functions and achieves asymmetric properties. It is designed for broadcasting authentication in wireless ad-hoc networks.

B. Motivations

Wireless sensor networks [4], which is power consumption constrains and scalable to large scale of deployment, has been thoroughly studied as it brings the IoTs one step closer to reality. It can provide an autonomous and intelligent link between the virtual world and the physical world. The benefits of connecting both WSNs and other IoTs elements go beyond remote access, as heterogeneous information systems can be able to collaborate and provide common service [5]. Lots of elements in IoTs cooperate via WSNs, which let WSNs be called the skin of IoTs.

Many relevant areas of technology are critical in the evolution of the Internet of Things, in general, and of the Connected Vehicle, in particular. The development of VANETs [6] is from 'Vehicle to Vehicle' to 'Vehicle to Roadside', and until to 'Vehicle to Internet'. The evolving Connected Vehicle architecture and technology can be seen as one of the first and most exciting and motivating manifestations of IoTs.

If two networks want to communicate, but they do not have a uniform protocol, one critical problem in the network scenario is to make the hybrid network can change messages via a security channel [5].

Distributed network architecture is widely used in IoTs and some elements in it have limited memory [7]. In securing IoTs, source authentication is one critical problem, which enable receivers of broadcast data to verify that the received data really originates from the claimed source and was not modified on route. Consequently, not only tolerance of DoS attack is very important in broadcasting network, but also a source authentication protocol that can tolerate DoS attack and catch up with the energy-limitation requirements is needed in IoTs.

C. Related works

Alcaraz et al [5] focus on the security challenges of networks' integration that take place at the network level. The security challenges are the integration of security mechanisms and user's acceptance, data privacy and the protection of the components of the IoTs.

Rajani et al [8] apply cognitive security protocol that disseminates information using distributed sensor technology while prioritizing robustness against DoS attack in VANETs. The Intelligent Transportation System (ITS) uses wireless and mobile ad-hoc sensor network which has inspired many autonomous applications. However, the security protocol focuses on the DoS attack which is only associated with VANETs.

There are two extension versions of TESLA: TESLA++ [9] and μTESLA [10]. TESLA++ is a DoS resilient version of TESLA and is designed for VANETs. It can tolerate both computational-based and memory-based DoS attack. μTESLA is designed for WSNs and it can catch up with the energy-limitation requirements in WSNs.

D. Challenging issues

It is difficult to make broadcast secure [11], because: 1) packets may get lost, but many broadcast applications do not retransmit them; 2) receivers often need to process data as packets arrive, rather than buffering data; 3) receivers are heterogeneous, with widely varying bandwidth and computation resources; 4) the group of receivers may be dynamic, with members joining and leaving the group at any time. The four characters of a broadcast network show us that DoS attack is very likely to damage the network and expose broadcast messages to attackers.

978-1-4673-0937-0/12/$31.00 ©2012 IEEE

Both TESLA++ and μTESLA are modified from TESLA. However, there are several differences between the protocol TESLA++ and μTESLA. TESLA++ cannot catch up with the energy-limitation requirements in WSN. μTESLA cannot tolerate memory-based DoS attack. If one WSN needs to communicate with one VANET, for example, the road side WSNs is helpful for accident monitoring, there could be a security integration problem.

In hybrid WSN and VANET network, we need to broadcast authentication protocol that can tolerate DoS attack and catch up with the energy-limitation requirements.

E. Our contributions

Our motivations and the challenge issues have been mentioned before. The broadcasting protocol TESLA and its two extended versions are presented in section II. Our proposal follows in section III. Analysis of our proposal is shown in section IV before a conclusion in section V. The main contributions of our work are as follows:

1) Our proposal shows a favorable performance on resisting of both computational and memory-based DoS attack. The sender in our protocol sends Message Authentication Code (MAC) and an index number at first. Then as time delay, the sender sends the message accompanied by corresponding key.
2) Our protocol provides acceptable consumption during DoS attack-tolerant. We pre-distribute the one-way chain key generation algorithm instead of pre-distributing the key pool.
3) Under the assumed network scenario in IoTs, which requires the communication between WSNs and VANETs, our protocol provides a uniform protocol for source authentication.

II. Preliminaries

A. TESLA, TESLA++ and μTESLA

Recall that both TESLA++ and μTESLA are modified versions of TESLA. All the three protocols are introduced in this section as background.

The main idea of TESLA [3] is that the sender attaches to each packet a MAC computed with a key k known only to itself. The receiver buffers the received packet without being able to authenticate it. A short while later, the sender discloses k and the receiver can authenticate the packet. Consequently, a single MAC per packet suffices to provide broadcast authentication, provided that the receiver has synchronized its clock with the sender ahead of time.

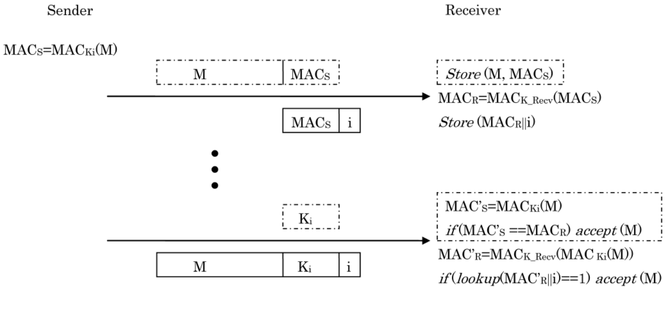

Fig. 1. Comparison between TESLA and TESLA++

TESLA is resilient to computational DoS attacks but vulnerable to memory-based DoS attack. To address such memory-based DoS attack in TESLA, TESLA++ [9] provides the same computationally efficient broadcast authentication as TESLA with reduced memory requirements.

Fig.1 shows the comparison between TESLA and TESLA++. Both sending and storing packets, which are boxed up by the dotted line, belong to TESLA. The other is TESLA++. In TESLA++, a receiver only stores a self-generated MAC to reduce memory requirements. Since receivers merely store an abbreviated version of the sender's data, the sender first broadcasts the MAC and later broadcasts the corresponding key and message. It is similar to the Guy Fawkes protocol [12]. Under TESLA++, both attacks on broadcasting MACs alone and attacks on storing shortened MACs are prevented without decreasing security. When storing only re-MACed values, the maximum memory consumption is a function of the maximum number of MACs which can be broadcasted in an interval and how long MACs are stored.

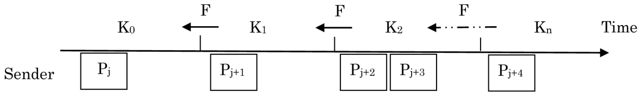

Fig. 2. Using a time-released key chain for source authentication in μTESLA

There will be a mishap if TESLA is used into WSN directly. Because in TESLA, the sender attaches to each packet a MAC computed with a key k. It is not accepted by WSN because a sensor node has limited space for message storing and limited energy for computation.

For resolving this problem, μTESLA [10] revises both key updating and initial part of authentication based on the original TESLA. Fig.2 shows an example of μTESLA. Each key of the key chain corresponds to a time interval, and all packets sent within one time interval are authenticated with the same key. The time until keys of a particular interval disclosed is two-time interval in this example.

The scalability of μTESLA is limited by its unicast-based initial parameter distribution, and it cannot resist DoS attacks. Multi-Level μTESLA [13] can resist to DoS attacks. The basic idea is to predetermine and broadcast the initial parameters required by μTESLA instead of unicast-based message transmission. To further improve the survivability of the Multi-Level μTESLA against DoS attacks, we can use redundant message transmissions and random selection strategies to deal with the messages that distribute key chain commitments.

Though the Multi-Level μTESLA [13] has nice properties on DoS tolerant and resistant, it is difficult to be implemented. Compared with the μTESLA, the Multi-Level μTESLA need more nodes memory and computing resources. Based on the different application scenario, it is better to select using parts of its security mechanism. Moreover, the Multi-Level μTESLA [13] only assume each message is from the base station to the sensor nodes. Broadcast messages from a sensor node to the sensor network can be handled as suggested in [14].

B. Broadcasting communication and DoS attack

A Denial of Service (DoS) attack is an explicit attempt to prevent the legitimate user of a service or data [15]. It makes the system or service unavailable for the user. Fig. 3 shows an example of the DoS attack. Hackers send a large amount of deceptions and requests to a server, which make the server not work normally in the near future.

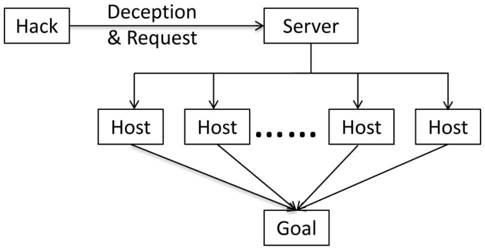

Fig. 3. DoS attack

Both WSNs and VANETs are distributed network, which change messages via broadcasting communication. Thus, an attacker can broadcast a large number of invalid malicious messages such that receivers expend an excessive amount of the memory resource as part of a 'pollution attack' [14].

WSNs do not generally adhere as closely to the TCP/IP protocol, which has five layers: physical, link, network, transport, and application [16]. The TCP/IP layer model is still useful for categorizing various DoS attacks and defense in WSNs. Due to consider the character of broadcast communication, we only focus on the DoS attack on the network, transport, and application layers. They are concluded in TABLE I.

TABLE I
DoS attacks at network, transport, and application layers in WSN

Protocol layer	Network	Transport	Application
Attacks	Spoofing, Replaying, Hello floods, Homing	SYN(synchronize) flood, Desynchronization attack	Path based DoS, Reprogramming attacks

In VANETs, DoS attack shall not be allowed to happen, where seamless life critical information must reach its intended destination securely and timely [17], [18]. In summary, there are three ways that the attackers may achieve DoS attacks, namely communication channel jamming, network overloading, and packets dropping. The three levels of DoS attacks are concluded in TABLE II.

TABLE II
DoS attacks in VANET

Level	**Attack**
Basic level	Overwhelm the Node Resources
Extended Level	Jamming the Channel
Distributed DoS(DDoS)	Launch attack from different locations

III. Our protocol

A. Network Scenario

According to TABLE I and TABLE II, certain types of DoS attacks focus on physical damage, corresponding techniques are proposed for preventing visible tampering and for mitigating overstimulating. We focus on the DoS attacks that exploit weaknesses in the network protocols and applications.

In Fig.4, the roadside WSN is in command of message detection. There is a kind of communication, which looks like interface communication, that: when vehicles or RSUs in the VANET receive some message from the WSN, they need to authenticate the source of the message. Otherwise, the VANET will be vulnerable to be attacked. However, if the message comes from the WSNs, whose nodes are different from the nodes in VANET. The nodes in WSNs have a limitation on energy consumption. Sensor nodes are lower power than the nodes in VANET. Thus, the original source authentication protocol TESLA++ for VANET is unsuitable for WSNs. Meanwhile, the μTESLA for WSN cannot tolerate DoS attacks. It is unsuitable for VANET.

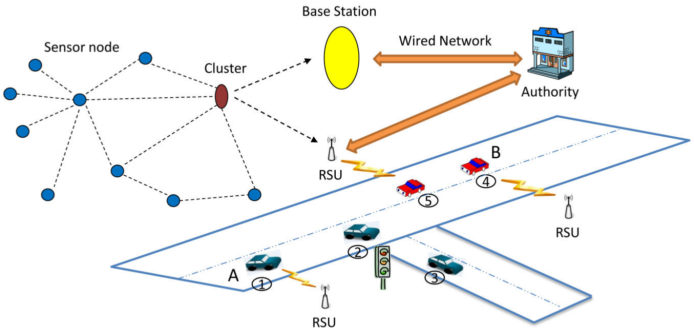

Fig. 4. The structure of network scenario in our proposal

B. Target of our protocol

The network scenario is different from gateway. Because a gateway is often used for routing protocols, and it is more biased to engineering. The target of our protocol is to prevent DoS attack and let WSN communicate with VANET in some fraction of the time. The roadside WSN does not need to communicate with the VANET always. If our protocol can prevent DoS attack when the WSN communicates with the VANET, it will be acceptable. Our protocol is not only for guaranteeing the interface can work normally, but also helpful for the authentication in each independent network.

The original TESLA can tolerate only computational DoS attack. The target of our proposal is planning to tolerate and resist not only the computational DoS attack, but also the memory-based DoS attack. Thus, we revise the sequence of packets sending. A sender sends MAC first and then sends message together with key after time delay, the receiver need not to store the message, whose size is bigger than both MAC and message. This part is revised from the TESLA++.

A VANET requires seamless message exchanging. As scale of network enlarged, the one level key chain in μTESLA becomes longer, which will bring expensive cost to the VANET. Our proposal provide two-level key chain instead of that structure. The details of this structure are presented in next subsection.

C. Structure of our protocol

In Fig.5, time advances left-to-right. Key K_i is used for the high-level time interval I_i, and $K_{(i,n)}$ is used for the low-level time interval $I_{(i,n)}$. F_0, F_1 and F_{01} are three different pseudo random functions, anybody can compute forward but nobody can compute backward.

- *Setup:* Before packets sending, F_0, F_1 and F_{01} have been pre-determined to the sender. The sender generates

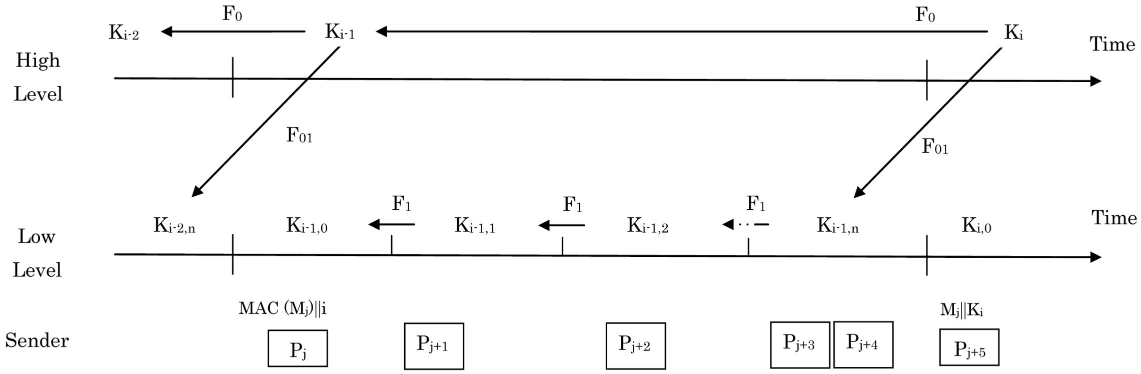

Fig. 5. The two level key chains in our scheme

the last key K_i of a high-level key chain by randomly. The previous keys in the high-level key chain will be generated via K_i by F_0. Time is split into time intervals of uniform duration I_i in high-level and $I_{(i,n)}$ in corresponding low-level. During I_i, the key $K_{(i,n)}$, which is used in the corresponding low-level key as the last key, is generated via K_i by F_{01}. The previous keys in the low-level key chain is generated via $K_{(i,n)}$ by F_1. The delay of time for release of key is set up as $d \times I_i$ in high-level and for release of key and message is set up as $d \times I_{(i,n)}$ in low-level. d is the number of uniform time interval. The high-level key chain and the low-level key chain have different functions. Their explanation are followed.

- *Two-level key chain:* Note that high-level key chain only predetermines and broadcasts the key chain commitments. The high-level key chain is used to authenticate the commitment of each low-level key chain. The high-level key chain uses a long fairly interval to divide the time line so that it can cover the lifetime of a sensor network without having too many keys. The low-level key chains have short enough intervals so that the delay between the receipt of broadcast messages, and the verification of the messages is tolerable. Thus, the two-level protocol has the same degree of security as μTESLA.
- *Low-level key chain:* Because the low-level keys are not entirely chained together, losses of a key disclosure message for upcoming keys in a low-level key chain cannot be recovered. For resolving this problem, each $K_{i,n}$ is derived from a high-level key K_{i+1} through the pseudo random function F_{01}. That is, $K_{i,n} = F_{01}(K_{i+1})$. As a result, the loss later keys in a low-level key chain can be recovered from by the keys from the high-level key chain.
- *Broadcast messages:* In order for the sender to use the n size low-level key chain in the interval I_i, the last key $K_{i,n}$ of the low-level key chain need to be authenticated before the time interval beginning. After authentication of the $K_{i,n}$, to broadcast the message M_j and the key in the interval $I_{(i,0)}$, the packet P_j which includes the $\{MAC_{K_{(i,0)}}(M_j) \parallel i\}$ should be sent in the interval $I_{(i-1,0)}$. Here, '||' means concatenation. Because of the sequence number i in each message, replay attacks can be easily defeated.
- *Authenticate messages:* To authenticate message M_j, the sender first broadcasts the $MAC_{K_{(i,0)}}(M_j)$ which is computed with the key $K_{(i,0)}$, along with the key index i. Upon reception, using the key index i and the time associated with the start of the sender's key chain, a recipient first verifies the security condition to ensure that the key $K_{(i,0)}$ for the sender has not yet been broadcasted and is thus only known by the sender. Over time, the receiver will store more MAC and key index in memory. When a stored MAC successfully authenticates a message, the receiver can free the memory used to store the MAC and key index.

IV. Security and Performance Analysis

In this part, both security analysis and performance analysis are provided. In the security analysis part, analysis on tolerance of computational DoS attack and memory-based DoS attack is presented, following by the comparison between our proposal and the other three protocols under the aforementioned hybrid-vehicle-sensor network scenario. In the performance analysis part, the discussion on number of buffers and the degree of bandwidth tolerance on forge messages are discussed. Some rough calculations demonstrate the memory savings and Dos attack tolerate of our protocol.

A. Computational DoS attack

The computational DoS attack mainly comes from attacks on broadcasting MACs alone.

If an attacker waits until the key and message are broadcasted, the attacker will try to find a different message M' which results in the same MAC as the original sender's message M (e.g. $MAC_{K_i}(M) == MAC_{K_i}(M')$).

However, generation of such a message implies the underlying MAC was not Chosen Message Attack (CMA) secure. Moreover, to discover an undisclosed key K_i, an attacker must defeat the one-way property of the hash chain which is computationally infeasible. Thus, the probability of success for the attacks on broadcasting MACs alone is negligible.

B. Memory-based DoS attack

The memory-based DoS attacks mainly come from attacks on storing shortened MACs and the ability of maximum storage.

For the attacks on storing shortened MACs, our protocol, which has small time intervals and relatively small receiver

MACs, provides a negligible probability that an attacker can spoof another sender as a result of the storage optimizations.

For the ability of maximum storage, we discuss the upper-limit on memory consumption in different hybrid-vehicle-sensor networks. In the case of a bandwidth of 56Mb/s, a 100ms time interval, and an 80bit sender MAC, an attacker needs to send about 70 thousand MACs in an interval. On the other hand, the real time requirement in VANETs reduces the maximum number of the stored MACs to less than the maximum number that could be broadcasted in certain time intervals [19]. Thus, it is difficult to attack successfully without enough time.

Moreover, for example, if broadcast MACs are 80bit, the re-MACs by receiver will be just 24bit long. The receivers at most need to reserve less than 1/2 space. This re-MACs could help for saving more space and make the memory-based DoS attack more difficult.

C. Compared with TESLA, TESLA++ and μTESLA

μTESLA cannot tolerate both computational and memory-based attack. Moreover, as the scale of network enlarges quickly, μTESLA need more space to store longer key chain and more time consuming during its initial step because of its unicast characters. Even though TESLA++ can tolerate both DoS attacks, it costs higher power consumption because it needs space to update and share the key pool not only the key generation algorithm. Compared with μTESLA and TESLA++, our proposal can resist both computational and memory-based attack with lower power consumption.

In TESLA and μTESLA, we know that an attacker may send a large amount of forged messages to exhaust the nodes' buffer before they can authenticate the buffered messages and force them to drop some authentic messages. After filtering out this kind forged messages, our proposal provides a random selection method to improve the reliable broadcast of messages.

It is worth mentioning that a broadcast authentication protocol has a prerequisite for secure: no attacker can forge the correct packet. If the prerequisite is satisfied, the protocol can be accepted. All the four schemes are designed based on this prerequisite. The conclusions of the comparison among the different properties of these source authentication protocols are shown in TABLE III.

In the initial step of authentication, TESLA and TESLA++ used digital signature for obtaining the initial key and time synchronization. Even if Elliptic Curve Digital Signature Algorithm (ECDSA) [9] provide fast authentication and non-repudiation, using digital signature for the initialization is computationally expensive. μTESLA and our protocol use Secure Network Encryption Protocol (SNEP) [10] for the initialization. SNEP is based on pre-sharing the master key, which provides lower computation consumption.

Incidentally, the one-way chain [3] is used in our protocol for key generation. Compared with TELSA++, our protocol does not need to store key pool. If new nodes add in, key updating will be needed for not disclosing the secure packets. During key updating, TESLA and TESLA++ need to update the key pool. It means the complexity of their key updating is $O(n)$. Meanwhile, μTESLA and our protocol only need to update the initial key and the size of key chain. It means the complexity of key updating is $O(2)$. Our protocol reduces the complexity obviously, which is helpful for reserve energy during communication.

D. Performance analysis

For quantifying the probability of successful authentic copy and frequency of forge a message, we present the following two definitions:

Definition 1: The probability of forged copies p is defined as $\frac{k(forgedpackets)}{n(totalpackets)}$, while $n(totalpackets)$ denotes the number of total packets and $k(forgedpackets)$ denotes the number of forge packets. Assume there is a single buffer, the probability that a sensor node has an authentic copy is $P = 1 - p$. Assume there are m multiple buffers, the $P = 1 - p^m$. That is:

$$P = \begin{cases} 1 - p & m = 1 \\ 1 - p^m & m > 1 \end{cases}.$$

Definition 2: Let B_d, B_a, B_f denote the fraction of bandwidth, which is used by data, authentic messages, and forged messages, respectively. Assume each message has the same probability p' of being lost in the communication channel. To simplify the analysis, we assume an attacker uses all available bandwidth to launch a DoS attack. Thus, we define $B_d + B_a + B_f = 1$.

To ensure the probability is at least P, we have

$$1 - \left(\frac{B_f \times (1 - p')}{B_a \times (1 - p') + B_f \times (1 - p')}\right)^m \geq P.$$

As $B_d + B_a + B_f = 1$, we have

$$B_a \geq (1 - B_d)(1 - \sqrt[m]{1 - P}).$$

The number of buffers m is based on the resource on sensor nodes. The bandwidth for data packets B_d is based on the predictable application behaviors. The probability P of a sensor node is based on the expected security performance under severe DoS attacks. If we can determine the m, B_d and P, we can compute B_f and then determine the frequency of messages. Moreover, we may examine different choices of these parameters and make a trade-off most suitable for the hybrid networks.

To ensure 90% of low-level key chain commitments are authenticated before the key chain is used, we discuss the bandwidth requirements and the influence from the number of buffers. The corresponding figures are drawn in Fig. 6 and Fig. 7, respectively.

In Fig. 6, it shows that up to 90% of the bandwidth is required for authentication packets if there is only single buffer and few bandwidth for data packets. It means such a network scenario is facing aggressive attackers who try everything possible to disrupt the normal operation of the network.

However, as the bandwidth for data packets increasing, the bandwidth requirement for authentication packets decreased substantially. This is because when the data consume more bandwidth, there is fewer bandwidth for the DoS attacks. And the requirement for authentication packets is also reduced.

In Fig. 7, it shows that the increasing in the number of the buffers can reduce obviously the bandwidth requirement for authentication message's packets.

Moreover, Fig. 7 shows that the smaller m is, the more effective on B_a is.

TABLE III
COMPARISON OF THE DIFFERENT PROPERTIES AMONG SOURCE AUTHENTICATION PROTOCOLS

Scheme	DoS tolerance		Energy Consumption		
	Computation	Memory	Initialization	Traffic (key updating)	Storage (Receiver)
TESLA	OK	NO	Expensive (Digital signature)	$O(n)$	Store (M, MAC_S)
TESLA++	OK	OK	Expensive but fast (ECDSA)	$O(n)$	Store (MAC_R, i)
μTESLA	NO	NO	Efficient (SNEP)	$O(2)$	Store (M, MAC_S)
Our Protocol	OK	OK	Efficient (SNEP)	$O(2)$	Store (MAC_R, i)

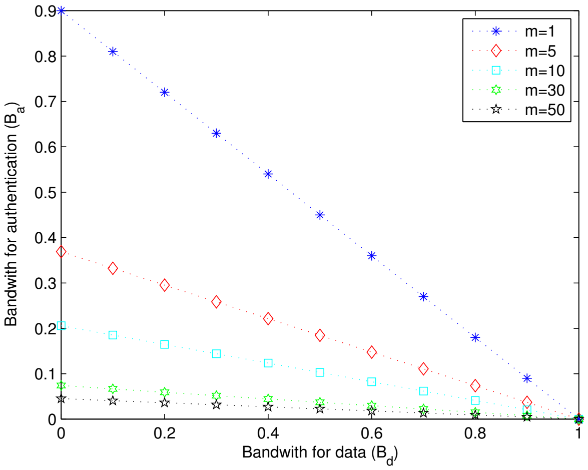

Fig. 6. Relationship between B_a and B_d for P=0.9

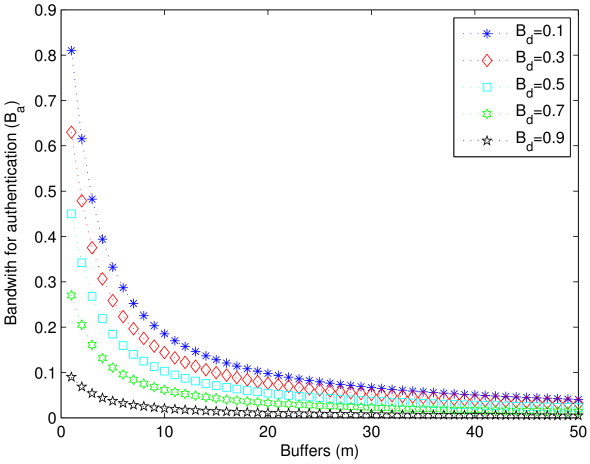

Fig. 7. Relationship between B_a and m for P=0.9

V. CONCLUSION

Our broadcast authentication protocol can tolerate both computational and memory-based DoS attack with low energy consumption. Our paper shows that independent TESLA, μTESLA and TESLA++ are unsuitable for the hybrid-vehicle-sensor networks. Toleration of DoS attack is a critical problem in a broadcast network such as Internet of Things. As some elements in this kind hybrid network are memo-limited, power constraints, our work brings certain promotion on source authentication protocol based on the original lightweight TESLA protocol.

ACKNOWLEDGMENT

The first author is supported by the governmental scholarship from China Scholarship Council.

REFERENCES

[1] INFSO D.4 Networked Enterprise and RFID INFSO G.2 Micro and Nanosystems, in co-operation with *the Working group RFID of the ETP EPOSS, internet of things in 2020: roadmap for the future*, 27 May, 2008.

[2] V. Ovidiu, et al. Internet of things strategic research roadmap, *European Commission -Information Society and Media DG*, 2009.

[3] A. Perrig, R. Canetti, J. D. Tygar and D. Song, The TESLA Broadcast Authentication Protocol, *RSA Laboratories*, vol. 5, no. 2, Summer / Fall 2002.

[4] I. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, Wireless sensor networks: a survey, *Computer Networks*,2002;38(4):393-422.

[5] C. Alcaraz, P. Najera, J. Lopez and R. Roman, Wireless Sensor Networks and the Internet of Things: Do We Need a Complete Integration?, *SecIoT 2010*.

[6] Keynote of the Eighth ACM International Workshop on VehiculAr InterNETworking (VANET 2011), *http://husky.crhc.illinois.edu/vanet2011/program.html*.

[7] Internet of Things: Strategic Research Roadmap, *European Commission - Information Society and Media DG*, September, 2009.

[8] R. Muraleedharan, et al, Cognitive security protocol for sensor based VANET using swarm intelligence, *The Asilomar Conference on Signals, Systems, and Computers (Asilomar)*, 2009.

[9] A. Studer, F. Bai, B. Bellur and A. Perrig, Flexible, Extensible, and Efficient VANET Authentication, *Journal of communication and networks*, 2009.

[10] A. Perrig, R. Szewczyk, V. Wen, D. Culler and J. D. Tygar, SPINS: Security protocols for sensor network, *Wireless Networks Journal (WINE)*, September 2002.

[11] A. Perrig, Security Protocols for Broadcast Networks, *Ph. D thesis, Department of Computer Science University of California*, Berkeley, Tuesday, February 5, 2002

[12] R. J. Anderson, F. Bergadano, B. Crispo, J.-H. Lee, C. Manifavas, and R. M. Needham. A new family of authentication protocols, *ACM Operating Systems Review*, 32(4):9-20, Oct. 1998.

[13] D. Liu and P. Ning, Multi-Level μTESLA: Broadcast Authentication for distributed sensor networks, *ACM Transactions on Embedded Computing Systems*, vol. 3, no. 4, November 2004, Pages 800-836.

[14] A. Perrig, R. Canetti, D. Song and J.D. Tygar, Efficient and Secure Source Authentication for Multicast, *Proceedings of Network and Distributed System Security Symposium*, California, USA, February 2001.

[15] D. K. Chaitanya, et al, Analysis of Denial-of-Service attacks on Wireless Sensor networks using simulation, *In Kaspersky Lab IT Security Conference for the Next Generation*, Erfurt, Germany, 27-30 January, 2011.

[16] D. R. Raymond, et al, Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses, *IEEE Pervasive Computing*, vol. 7, no. 1, January-March 2008.

[17] H. Hasbullah, et al, Denial of Service attack and its possible solutions in VANET, *World Academy of Science*, Engineering and Technology 65, 2010.

[18] J. M. McCune, E. Shi, A. Perrig and M. K. Reiter, Detection of Denial-of-Message Attacks on Sensor Network Broadcasts, *Proceedings of the 2005 IEEE Symposium on Security and Privacy*, Washington, DC, USA , 2005.

[19] Qing Li and Wade Trappe, Reducing Delay and Enhancing DoS Resistance in Multicast Authentication Through Multigrade Security, *IEEE Transactions on Information forensics and security*, vol. 1, no. 2, June 2006.