Authentication Protocol Using Error Correcting Codes and Cyclic Redundancy Check

C. Pavan Kumar[1] and R. Selvakumar[2(✉)]

[1] School of Computer Science and Engineering (SCOPE), VIT University, Vellore 632014, Tamil Nadu, India
pavankumarc@ieee.org
[2] School of Advanced Science (SAS), VIT University, Vellore 632014, Tamil Nadu, India
rselvakumar@vit.ac.in

Abstract. Authenticating devices in communication system is an important and challenging task. With many diverse devices getting connected to communicate, establishing authentication of such devices among themselves (or with a central server) is essential to overcome possible attacks in the communication channel and by adversaries. In this paper, an authentication protocol is proposed based on linear error correcting codes, pseudo random numbers and cyclic redundancy check function. General protocol is provided in this paper and can be used for any specific linear error correcting codes defined over finite field. The proposed protocol is resistant against replay attack, man-in-the-middle and impersonation kind of attacks. One of the advantages of the proposed protocol is that it can be incorporated within the framework of any communication system that uses linear error correction system to achieve reliability or can be implemented independently to achieve security in terms of authentication.

Keywords: Authentication protocol · Error correcting codes
Cyclic redundancy check

1 Introduction

With diverse devices getting connected to internet and communicate with each other (or with central server), it is necessary to have authentication protocols that ensure that the messages received from senders are trustworthy and genuine, and are not altered from intruders of network or jammers or attackers present in the communication channel [1,2]. In an environment that is prone to attacks, it is very important to establish authenticity of devices in communication system. Shannon's influential paper on Mathematical Theory of Communication has immensely influenced research in many directions [3]. The problems of achieving

S. Chellappan et al. (Eds.): WASA 2018, LNCS 10874, pp. 874–882, 2018.
https://doi.org/10.1007/978-3-319-94268-1_80

reliability and security in digital communication paradigm are addressed separately in literature. To achieve reliability error correcting codes are used rather than redundantly transmitting the same packets until an acknowledgment message is received from receiver. Additional parity bits are added to the message to be transmitted so that errors if any will be corrected by employing suitable decoding techniques. Adding such parity bits are little computationally expensive but provides better throughput over transmitting redundant packets repeatedly which incurs additional overhead. Encoding E can be given as an injective map as follows [4]:

$$E : \Sigma^k \rightarrow \Sigma^n \tag{1}$$

where, message m of length k is encoded into a message of length n over an alphabet Σ. The additional bits r added to message of length k are called parity bits or redundancy bits and $n = k + r$. Similarly, decoding D can be given as a function as follows [4]:

$$D : \Sigma^{n+\eta} \rightarrow \Sigma^k \tag{2}$$

where, η is the noise added by the communication channel.

To achieve security, efficient cryptographic techniques are used which are broadly classified into public key cryptosystem and private key cryptosystem. In public key cryptosystem, sender will possess a public key using which he/she encrypts the message and transmits. User upon receiving the encrypted message uses his/her private key to decrypt the message. In private key cryptosystem, both sender and receiver will agree upon a mutual set of keys that act as key to encrypt and decrypt. Sender using his/her private key, encrypts the message and transmits whereas receiver will use his/her private key to decrypt the message.

Encryption Enc can be given as a mapping from actual message defined over an alphabet to another message defined over different alphabet as follows:

$$Enc : \Sigma^n \rightarrow \sigma^n \tag{3}$$

where, Σ and σ are the alphabets over which plain text and cipher text are defined respectively. Similarly, decryption Dec is given as a map as $Dec : \sigma^n \rightarrow \Sigma^n$.

In this paper, we propose a multi purpose light weight authentication protocol based on coding theory, i.e., by exploiting the error correction capability of the code. Maurya et al. [5] have used such coding theory based authentication protocol to authenticate Radio-Frequency Identification (RFID) tags with the RFID readers with the help of a trusted server. In our proposed protocol the necessity of such server assistance is removed. This makes the proposed protocol suitable for use in diverse communication scenarios such as Device to Device (D2D), Machine-to-Machine (M2M), Vehicle-to-Vehicle (V2V), Cognitive Radio Networks (CRNs) and Cyber Physical Systems (CPS) that uses error correction codes for achieving reliability. In these communication setup, i.e., Device

to Device (D2D), Machine-to-Machine (M2M), Vehicle-to-Vehicle (V2V), both sender and receiver will have almost same capabilities (can be termed broadly as Ubiquitous computing [6]). The protocol is constructed using the techniques of coding theory especially linear error correcting codes that are defined over Field $\mathbb{F}_q^n$, pseudo random numbers and Cyclic Redundancy Check functions. General protocol is given in this paper and it can be used with any linear error correcting codes defined over $\mathbb{F}_q^n$. Here, the emphasis is on achieving authentication in communication systems exploiting error correction capability of the code employed to achieve reliability. Proposed method is also useful in achieving security in terms of authentication in communication systems that has only physical layer in the communication stack and not the upper layers [1,7] (in scenarios such as using TV spectrum as opportunistic cognitive radio [8,9]).

Present paper is organized as follows: In Sect. 2 related works and attack models are discussed. Section 3 discusses the proposed authentication protocol. Analysis of the proposed protocol is made in Sect. 4. Section 5 deals with conclusions and future work.

2 Related Works and Attack Models

2.1 Related Works

To overcome these challenges coding theory and cryptography techniques can be efficiently combined. The idea of employing error correcting codes for authenticating messages were introduced by Gilbert et al. [10]. The mathematical formulation of such schemes and a survey on construction of unconditionally secure authentication schemes from error correcting codes was given by Simmons [11,12]. There after many authentication schemes were proposed in the literature [13,14] to achieve security. Kacewicz [15] has analyzed few error correcting codes that are suitable to achieve reliability as well as security in the context of wireless communication systems.

Tsimbalo et al. [16–18] have exploited the Cyclic Redundancy Check (CRC) function bits of Bluetooth Low Energy (BLE) and IEEE 802.15.4 standards meant for resource constrained IoT devices intended to detect errors (not for correcting, as error correction or high level encoding involves processing overhead for the resource constrained devices), and proposed Forward Error Correction (FEC) over CRC which was purposefully disabled in those two protocols for saving energy at sender side. Tsimbalo et al. [16] proposed forward error correcting codes over such CRC redundant bits and checked the performance of such codes in communication paradigms where receiver can process received codewords from constrained devices and employ decoding to correct errors instead of discarding received packets and requesting sender to resend discarded packets.

Ez-zazi et al. [19] have proposed coding based reliable communication scheme for constrained IoT devices. The scheme uses Low Density Parity Check codes and CRC to achieve reliability. Sender will encode data sensed using LDPC codes and CRC of encoded data is computed, such encoding and CRC computation is termed as joint FEC/CRC by authors. Such encoded data is transmitted to the

next hop or base station, upon receiving the joint FEC/CRC encoded package, first CRC will be checked to find if there are any errors in the received packets, if not it will be transmitted further. If any errors are detected by CRC, then the received packet will be decoded using belief propagation technique of decoding LDPC codes and errors will be corrected. If such packet's error correction is performed at intermediate hops, then the message will be further encoded using LDPC scheme and further CRC is computed before transmitting it further.

Alabady et al. [20] have proposed novel Low Complexity Parity Check (LCPC) codes for the resource constrained IoT devices. The proposed scheme encodes the data using LCPC codes at sender and uses three stage decoding algorithm to correct up to two bit errors if any and decode the message. This scheme corrects only one bit and two bit errors and beyond that discards the received packet and request the sender to retransmit the discarded packet.

2.2 Attack Models

The common attacks both cryptographic and coding theory methods used to achieve reliability and security subjected to are - eavesdropping, Denial-of-Service attacks, intrusion attacks, man-in-the-middle attacks, replay kind of attacks. By combining or selectively using techniques from coding theory as well as cryptography, attacks such as intruder, Man-in-the-Middle, replay and Denial-of-Service can be effectively mitigated.

Intrusion Attack. In intrusion attack, the adversaries will join the network or the group of existing communication entities posing as legitimate user and then use the network resources or information similar to legitimate users or sometimes even dominating legitimate users. Mitigating or overcoming or detecting such intrusion is necessary to make network resources available only for legitimate users.

Man-in-the-Middle Attack. Communication between sender and receiver is through a channel that is subjected to noise and attacks. Additive White Gaussian Noise (AWGN) is considered in the channel that changes bits and the channel is assumed to be insecure. Any intruder posing as legitimate user can send messages to receiver and thwart communication. Identifying the source of received message at receiver is an important task to mitigate such attack.

Replay Attack. The communication between sender and receiver can be copied (copying session keys) and used at later instances. Such attacks should be avoided in real time communication systems so that entities will not function adversely.

Denial-of-Service Attack. Denial-of-Service attack will make legitimate users deprive of services. One instance of it is to use powerful signal and entirely change the routing of packets in the network to other unintended nodes than to

legitimate receiver present in the network. Also, making the receiver deprive of legitimate data over network is an instance of Denial-of-Service attack.

3 Authentication Protocol

The proposed protocol works in two phases, namely, initialization phase and execution phase. Initialization phase involves setting up of the environment necessary for execution of the protocol. Notations used in the protocol are given in Table 1.

Table 1. Notations

Notation	Description
K	Shared secret key
$\mathbb{C}$	Linear error correcting code over $\mathbb{F}_q^n$
c_i	Codeword $c_i \in \mathbb{C}$
CRC	Cyclic redundancy check sum
R_s	Random number generated at sender
R_r	Random number generated at receiver
$\|\|$	Concatenation operation
$\oplus$	XOR operation

3.1 Assumptions

The following assumptions are made in defining the protocol.

1. $[n, k, d]_q$ error correcting code is assumed, where n is the length of the codeword, k is the information to be encoded, d is the minimum Hamming distance and q is the alphabet over which code is defined [21]. The error correcting code $\mathbb{C}$ is assumed to have 2^k distinct codewords.
2. It is assumed that the random number generated at the sender R_s is such that $wt(Rs) \leq t$, where t is the error correction capacity of the code. It is to ensure that the errors that occur in this can only be corrected (Hamming bound).
3. The length of pseudo random numbers R_s and R_r are assumed to be n, which is same as the length of the codeword $c \in \mathbb{C}$.

3.2 Initialization Phase

In the initialization phase, both sender and receiver will compute functions that are necessary for the working of the protocol. Both sender and receiver will share a secret key K, also called as shared secret key. Both sender and receiver will have respective pseudo random number generators that can generate pseudo random numbers indicated by R_s and R_r respectively. But the pseudo random

generator at the sender can generate random number which satisfies the condition that $wt(R_s) \leq t$. Both sender and receiver will have their respective Cyclic Redundancy Check (CRC) functions that computes the CRC sums for the inputs provided. The encoder function of sender will encode message m of length k into codeword c of length n.

3.3 Execution Phase

Both sender and receiver will compute S_s and S_r respectively by XOR-ing random number generated with the shared secret key K. $S_s = R_s \oplus K$ and $S_r = R_r \oplus K$. Both sender and receiver will exchange S_s and S_r. At receiver, random number of sender R_s will be computed by XOR-ing the received S_s values with the shared secret key K, i.e., $R_s = S_s \oplus K$. Similarly, sender will compute $R_r = S_r \oplus K$ to get R_r. Thus, both sender and receiver will get R_r and R_s respectively without being explicitly sharing it.

Sender will concatenate the codeword c_i to be transmitted with the random number generated by both sender and receiver and compute CRC sum of the concatenated message, i.e., $CRC(c_i||R_s||R_r)$. Also, the sender will compute $c_i \oplus R_s$. Sender will transmit both $CRC(c_i||R_s||R_r)$ and $c_i \oplus R_s$ to the receiver. Let $E_1 = CRC(c_i||R_s||R_r)$ and $E_2 = c_i \oplus R_s$. E_2 will be similar to codeword.

Receiver will receive messages E_1 and E_2 from the sender. It will decode the received message E_2 employing Maximum Likelihood decoding as $R_s \leq t$ and produce codeword c_i'. Further, the receiver will compute E_3 such that $E_3 = CRC(c_i'||R_s||R_r)$. If E_1 computed at sender is equivalent to E_3 computed at receiver, i.e., $E_1 = E_3$ then the communication is authentic and it is sent from genuine sender, if not, i.e., $E_1 \neq E_3$ then message is being received from other sources than the intended sender. E_1 can be shared with the receiver as private key similar to that of Private Key Cryptosystem. Overview of the proposed Authentication protocol is given in Fig. 1.

Sender		Receiver
Shared Secret Key K		Shared Secret Key$K$
Random Number R_s		Random Number R_r
Compute $S_s = R_s \oplus K$		Compute $S_r = R_r \oplus K$
	$\xrightarrow{S_s}$	
	$\xleftarrow{S_r}$	
Compute $R_r = S_r \oplus K$		Compute $R_s = S_s \oplus K$
$E_1 = CRC(c_i\|\|R_s\|\|R_r)$		
$E_2 = c_i \oplus R_s$		
	$\xrightarrow{E_1}$	
	$\xrightarrow{E_2}$	
		Decode E_2 as c_i
		$E_3 = CRC(c_i'\|\|R_s\|\|R_r)$

Fig. 1. Proposed authentication protocol

4 Analysis of Proposed Authentication Protocol

4.1 Replay Attack

Adversary or intruder of the channel tries to send the same session details in a future instance to communicate with the receiver. But in the proposed protocol even if shared secret key K is known to the intruder, it is difficult to guess the random numbers R_r and R_s generated at receiver and sender respectively, as they will be generated for each session. CRC computed at both sender as well as at receiver further makes it difficult even if intruder knows either R_s or R_r as they will be freshly generated.

4.2 Impersonation Attack

If intruder stores E_2 and tries to use it in future instance proposed protocol will reject it as values of R_r and R_s will be generated for sessions or as and when required. Further, CRC will be computed at both sender and receiver. That makes it difficult for intruders to impersonate the sessions. Even though E_2 look like codeword it will be XOR-ed with R_s thus impersonating codeword is also difficult.

4.3 Man-in-the-Middle Attack

Intruder in the channel can alter the message E_2 in the channel and transmit. But due to the nature of generating S_s, S_r, E_2 and E_1 it will be easy to detect unauthenticated transmissions received and reject them.

4.4 Computation Cost

Three $\oplus$ – operations are performed at sender to compute S_s, R_r and E_1. Similarly, two $\oplus$ – operations are performed at receiver to compute S_r and R_s respectively. One time CRC operation is performed at sender as well as receiver. Both sender and receiver will perform two $||$ operation. If computation time to perform $\oplus$ operation is indicated by $T_{\oplus}$, CRC operation by T_{CRC} and $||$ operation by $T_{||}$, then computation time taken at the sender to implement the proposed protocol is $3T_{\oplus} + 2T_{||} + 1T_{CRC}$. This computation is in addition to the computation time required at the sender to compute codeword $c \in \mathbb{C}$. Similarly at the receiver it takes a total of $2T_{\oplus} + 2T_{||} + 1T_{CRC}$ to implement the proposed protocol in addition to the cost involved at receiver to decode the received codeword c' using Maximum Likelihood Decoder.

5 Conclusion

A simple authentication protocol is proposed in this paper based on linear error correcting codes, pseudo random number generators and CRC function. The proposed protocol provides resistance against replay attack, impersonation attack

and man-in-the-middle kind of attacks. The protocol can also be employed in any communication setups that uses linear error correcting codes (to achieve reliability) as discussed in paper to achieve security in terms of authentication. Further, it is interesting to incorporate this protocol in real time systems and analyze its performance.

References

1. Harrison, W.K., Almeida, J., Bloch, M.R., McLaughlin, S.W., Barros, J.: Coding for secrecy: an overview of error-control coding techniques for physical-layer security. IEEE Signal Process. Mag. **30**(5), 41–50 (2013)
2. Mukherjee, A., Fakoorian, S.A.A., Huang, J., Swindlehurst, A.L.: Principles of physical layer security in multiuser wireless networks: a survey. IEEE Commun. Surv. Tutor. **16**(3), 1550–1573 (2014)
3. Shannon, C.E.: A mathematical theory of communication. Bell Syst. Tech. J. **27**(3), 379–423 (1948)
4. Sudan, M.: Coding theory: tutorial & survey. In: Proceedings of the 42nd IEEE Symposium on Foundations of Computer Science, pp. 36–53. IEEE (2001)
5. Maurya, P.K., Pal, J., Bagchi, S.: A coding theory based ultralightweight RFID authentication protocol with CRC. Wirel. Pers. Commun. **97**(1), 967–976 (2017)
6. Friedewald, M., Raabe, O.: Ubiquitous computing: an overview of technology impacts. Telemat. Inform. **28**(2), 55–65 (2011)
7. Liu, Y., Chen, H.H., Wang, L.: Physical layer security for next generation wireless networks: theories, technologies, and challenges. IEEE Commun. Surv. Tutor. **19**(1), 347–376 (2017)
8. Nekovee, M.: Cognitive radio access to TV white spaces: spectrum opportunities, commercial applications and remaining technology challenges. In: 2010 IEEE Symposium on New Frontiers in Dynamic Spectrum, pp. 1–10. IEEE (2010)
9. Rempe, D., Snyder, M., Pracht, A., Schwarz, A., Nguyen, T., Vostrez, M., Zhao, Z., Vuran, M.C.: A cognitive radio TV prototype for effective TV spectrum sharing. In: 2017 IEEE International Symposium on Dynamic Spectrum Access Networks, DySPAN, pp. 1–2. IEEE (2017)
10. Gilbert, E.N., MacWilliams, F.J., Sloane, N.J.: Codes which detect deception. Bell Labs Tech. J. **53**(3), 405–424 (1974)
11. Simmons, G.J.: Authentication theory/coding theory. In: Blakley, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 411–431. Springer, Heidelberg (1985). https://doi.org/10.1007/3-540-39568-7_32
12. Simmons, G.J.: A survey of information authentication. Proc. IEEE **76**(5), 603–620 (1988)
13. Moulin, P., Koetter, R.: Data-hiding codes. Proc. IEEE **93**(12), 2083–2126 (2005)
14. Schillewaert, J., Thas, K.: Construction and comparison of authentication codes. SIAM J. Discret. Math. **28**(1), 474–489 (2014)
15. Kacewicz, A.: Coding Theory for Security and Reliability in Wireless Networks. Cornell University, Ithaca (2010)
16. Tsimbalo, E., Fafoutis, X., Piechocki, R.J.: CRC error correction in IoT applications. IEEE Trans. Ind. Inf. **13**(1), 361–369 (2017)
17. Tsimbalo, E., Fafoutis, X., Piechocki, R.: Fix it, don't bin it!-CRC error correction in Bluetooth low energy. In: 2015 IEEE 2nd World Forum on Internet of Things, WF-IoT, pp. 286–290. IEEE (2015)

18. Tsimbalo, E., Fafoutis, X., Piechocki, R.J.: CRC error correction for energy-constrained transmission. In: 2015 IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications, PIMRC, pp. 430–434. IEEE (2015)
19. Ez-zazi, I., Arioua, M., El Oualkadi, A., El Assari, Y.: Joint FEC/CRC coding scheme for energy constrained IoT devices. In: Proceedings of the International Conference on Future Networks and Distributed Systems, p. 18. ACM (2017)
20. Alabady, S.A., Salleh, M.F.M., Al-Turjman, F.: LCPC error correction code for IoT applications. Sustain. Cities Soc. (2018). https://doi.org/10.1016/j.scs.2018.01.036
21. Moon, T.K.: Error Correction Coding: Mathematical Methods and Algorithms. Wiley, Hoboken (2005)