Provably Secure Group Authentication and Key Agreement for Machine Type Communication Using Chebyshev's Polynomial

Probidita Roychoudhury, Basav Roychoudhury, Dilip Kumar Saikia

PII: S0140-3664(17)31091-5
DOI: 10.1016/j.comcom.2018.06.005
Reference: COMCOM 5714

To appear in: *Computer Communications*

Received date: 14 October 2017
Revised date: 25 February 2018
Accepted date: 13 June 2018

Provably Secure Group Authentication and Key Agreement for Machine Type Communication Using Chebyshev's Polynomial

Probidita Roychoudhury[a,*], Basav Roychoudhury[b], Dilip Kumar Saikia[c]

[a] *National Institute of Technology Meghalaya, Shillong -793001, Meghalaya, India*
[b] *Indian Institute of Management Shillong, Shillong -793014,Meghalaya, India*
[c] *Tezpur University, Tezpur- 784028, Assam, India*

Abstract

While the current cellular networks are optimized only for Human to Human, or Human Type Communication (HTC), the future generation of cellular networks foresees a rapid growth in the quantum of Machine Type Communication (MTC) i.e., communication among heterogeneous entities without the involvement of any human entity which can be seen in different Internet of Things(IoT) applications. A significant issue in Machine Type Communication is the presence of large numbers of communicating devices overloading the network with their signaling messages. This overload can have negative impacts in terms of delays and termination of security procedures, like authentication, affecting both HTC and MTC. In this paper, we propose a group authentication and key agreement protocol using Extended Chebyshev's Chaotic Map. The proposed protocol provides an efficient, in terms of reduced signaling traffic generated during the authentication procedure, and provably secure method for authenticating a group of MTCDs by the core network. The security analysis of the proposed protocol shows that it is secured against various threats like man-in-the-middle, replay attack etc.

Keywords: MTC, LTE-A, Chebyshev's polynomial, group authentication, security, IoT

[*] Corresponding author

Email addresses: probidita.roychoudhury@nitm.ac.in (Phone : +919089024278) (Probidita Roychoudhury), brc@iimshillong.ac.in (Basav Roychoudhury), dks@tezu.ernet.in (Dilip Kumar Saikia)