A

Dissertation

On

Light Weight One Way Cryptographic Hash Algorithm for Wireless Sensor Network

Submitted in Partial Fulfillment of Requirement

For the Award of the Degree of

Master of Technology

in

Computer Science and Engineering

by

Manoj Kumar

University Roll No. 2K12/CSE/27

Under Esteemed Guidance of

Vinod Kumar

Associate Professor, Computer Engineering Department, DTU

2015

Delhi Technological University

Delhi-110042, India

ABSTRACT

Authentication of a message is a great research challenge in today's advanced wire and wireless communication. Cryptographic hash functions are used to protect the authenticity of information. Some of the most popular and commonly used cryptographic hash algorithms are MD5 and SHA1. These hash algorithms are used in a wide variety of security applications e.g. securing node/message in traditional networks.

However, the commonly used hash algorithms require huge computational overhead which is not affordable by applications in energy-starved network e.g. wireless sensor network (WSN). In these applications the major constraints are communication, computation and storage overheads; out of which communication and computation overheads consume high energy. Keeping this fact in mind, in this work, a light-weight, one-way, cryptographic hash algorithm is suggested with a target to produce a hash-digest with fixed and relatively small length for such an energy-starved wireless network. The primary focus is making the algorithm light-weight so that upon using it in application of network like WSN, the nodes can successfully run the algorithm with low energy. It is suggested that such algorithm must fulfill all the basic properties such as preimage resistance, collision resistance of a one-way hash function. The proposed algorithm is developed using NS2 simulation tool and results were compared with MD5 and SHA1.

ACKNOWLEDGMENT

I take this opportunity to express my sincere gratitude to all those who have been instrumental in the successful completion of this project for their invaluable efforts, supports and encouragements.

I am deeply indebted to my mentor, **Mr. Vinod Kumar,** Associate Professor who has always guided me for successful completion of this project from the beginning of my study till the end. I am deeply indebted to him for the support, advice and encouragement he provided without which the project could not have been a success.

I would also like to express my sincere thanks to **Mr. R. K. Yadav,** Assistant Professor, who helped and inspired me at several occasions. His support is highly appreciated.

I wish to thank, **Mr. Manoj Kumar,** Associate Professor who helped make me to learn the basic concepts of Security and Cryptography and in several other ways.

I am grateful to **Prof. O.P.Verma,** HOD, Computer Engineering Department, DTU for his immense support. I would also like to acknowledge Delhi Technological University Library and staff for providing the right academic resources and environment for this work to be carried out.

Last but not the least I would like to express sincere gratitude to my parents and friends for constantly encouraging me during the completion of work.. Surely it is almighty's grace to get things done fruitfully.

Manoj Kumar
Roll No. 2K12/CSE/27
M.Tech (Computer Science & Engineering)
Department of Computer Engineering
Delhi Technological University
Delhi-110042

CERTIFICATE

This is to certify that the project report entitled **"Light Weight One Way Cryptographic Hash Algorithm for Wireless Sensor Network"** is a bonafide record of work carried out by **Manoj Kumar (2K12/CSE/27)** under my guidance and supervision in partial fulfillment of the requirement for the award of the degree of Master of Technology in Computer Science & Engineering from Delhi Technological University, Delhi. The matter embodied in this report has not been submitted for the award of any other degree.

Vinod Kumar
Associate Professor
Department of Computer Engineering
Delhi Technological University
Delhi-110042

Table of Contents

List of Figures