Table of Contents

1 Introduction 1

1.1 Problem Definition 2

1.2 Proposed Solution Overview 3

1.3 Existing Security Overview 4

1.3.1 μ TESLA 4

1.3.2 LEAP 5

1.3.3 RM - μ TESLA 5

1.4 Motivation behind the New Technique 6

2 Overview of Sensor Network 7

2.1 Feature and Requirements 7

2.2 Network Architecture 8

2.3 Differences between WSN and MANET 10

2.4 Sensor Network Applications 13

2.4.1 Disaster/Crime Prevention and Military Applications 14

2.4.2 Environmental Applications 14

2.4.3 Home Applications 14

2.4.4 Industrial Applications 15

3 Overview of Security Issues in Sensor Network 16

3.1 General Study of Security Issues 16

3.1.1 Traffic in Sensor Network 16

3.1.2 Security Requirements 19

3.1.3 Attack and Attacker 22

3.1.4 Security Classes 24

3.1.5 Threat Models 25

3.2 Overview of Attacks & their Security Approaches 26

3.3 Classification of Attacks against WSN 34

4 Overview of the Protocol CHEESPSN 35

4.1 Protocol Description 35

4.2 Possible Attack on the Protocol 36

5 Overview of the Implementation of CHEESPSN 38

5.1 nesC Language 38

5.2 TinyOS 41

6 Proposed Security Solution for Protocol CHEESPSN 43

6.1 Proposed Method 43

6.1.1 Proposed Algorithm 43

6.1.2 Proposed Code Hopping Technique 46

6.2 Security Analysis 47

6.3 Cost Analysis 50

6.3.1 Computational Cost 50

6.3.2 Communication Cost 50

6.3.3 Storage Requirement 51

7 Conclusion and Future Work 52

8 References 53

List of Figures and Tables

Fig 1: Architecture of a Sensor Network 10

Fig 2: Sensor information forwarding with and without clustering and aggregation 19

Fig 3: Classification of Attackers 24

Fig 4, 5 and 6: Spoofed, altered or replayed routing information Attack 28

Fig 7 and8: Selective Forwarding Attack 29

Fig 9: Sinkhole Attack 30

Fig 10: Sybil Attack 30

Fig 11: HELLO Flood 31

Fig 12: Sniffing Attack 32

Fig 13: Node Replication Attack 33

Fig 14: nesC Interface 40

Fig 15: nesC Components 40

Fig 16: An example mapping of data blocks to time slots 46

Table 1: Shows the summarized report of the differences between WSN and MANET 13

Table 2: Classification of attacks against WSN 34

List of Variables

K_i	Node Specific Private Key
K_b	Base Station Key
$K_{i,b}$	Key generated by XOR'ing K_i and K_b
h()	One way Hash function
T_p	Transmission Power
d	Distance
ID#	Id number of a sensor node