EXECUTIVE SUMMARY

Final Report of the Major Research Project

PROJECT TITLE:

Trust Based Authentication Mechanism for Mobile Ad-Hoc Network

ज्ञान-विज्ञान विमुक्तये

University Grants Commission
New Delhi

UGC Ref. No.: F. No. 42-128/2013 (SR) , Dt., 14-03-2013

Submitted By

Dr. S. Sivagurunathan
Assistant Professor
Principal Investigator
UGC - Major Research Project

Department of Computer Science and Applications
The Gandhigram Rural Institute (Deemed to be University)
Gandhigram - 624 302
Dindigul, Tamil Nadu, India.

1. Objectives of the project:

The research work has started with first and foremost queries that how to ensure an authentication of a node/soldier by the way it can cooperate well and how to make nodes become more trustworthy and how to make secure routing, so that, successfully complete a task in MANET based military environment. As a result of the queries, many security schemes have been studied.

Security mechanisms that have been proposed already are effective and mostly based on Shared Secret, Public Key Infrastructure (PKI), Digital Signature, Digital Certificate, Intrusion Detection Systems (IDS) and Hash functions. However, these techniques are centralized, pre-determined depend on trusted third party thereby increasing computation power, memory, consumption of communication bandwidth and battery power and performance degradation in overall network's throughput, availability and robustness as MANET has resource constrained nodes. The objective of the research work is to provide efficient, effective, scalable and light weight authentication schemes that provide integrated solution that leads to secure the MANET based military environment.

2. Achievements from the project:

The greatest achievement of the project is the successful development of trust-based security models for MANET based Military environment. It can be used to ensure the identity of participating nodes by excluding the untrusted nodes from MANET environment by the way authentication of nodes could be ensured. In addition, the development of trusted routing protocol could ensure the secure path while transmitting information from source to destination. Typically, military environments are dealing with highly sensitive information. In addition, imperfection may result in the loss of human life. Hence, with the help of this models and protocol, a military environment can ensure the security so that successful completion of mission.

3. Contribution to the Society:

The growing advancement of information and communication technologies open a gateway for many significant applications in India that also reflects in military environment. In

recent years, Indian army has well equipped with information and communication technologies and have tie up many software companies in order to provide the secure communication system in battle field environment. Among various technologies, MANET provide significant role in battled filed environment because of unique characteristics. However, such special characteristics lead to various security related issues.

In military, communication should be carried out on time and without loss of data so that successful completion of mission. The MANET enabled military equipment are always working well at the time of battle however due to its special characteristics such as limited battery power, open wireless nature and resourced constrained nature, the devices may loss their own control and become selfish. Therefore, to identify such type of devices in military environment, our trust-based models can be used.

Hence, the contribution to the society is in term of providing security by identifying untrusted soldiers and create a secure path while communication in MANET based military environment in India.

The main advantage is, security models that have been developed in these models are light weight hence it increases the life time of devices in terms of saving battery power and other resource. Therefore, the survival of soldiers in such environment can also be increased.

4. Summary of findings:

The development of security models comprises the following major things. Every model has its own role in terms of identifying the untrusted nodes but the overall whole is to ensure the authentication and guarantee the trust path. The summary of findings is herein:

Identifying the suitable routing protocol for military environment through case study and simulation

Every routing protocol in network environment has its own advantages as well as disadvantages. As military environment always owns highly confidential information, identification of right routing protocol for such application is important. Because suitability of routing protocol for one application may not suitable for other application. With this consideration in mind the initial work has been started.

Trust and Q-Learning based Security model (TQS)

This model is used to detect the untrusted nodes over Ad Hoc On Demand Distance- Vector (AODV) routing protocol. Here the untrusted nodes could be identified and eliminated by

calculating an aggregated reward, based on the Q-learning mechanism by using their historical forwarding and responding behaviour by the way authentication could be achieved.

A Centralized Trust Computation Model (CTC)

This model is used to ensure authentication based on own experiences, recommendations, social and sense making trusts of team members evaluated by commanders that create an efficient and secure team based on stereotypes model and prior direct trust will be evaluated between all the team members based on the number of successful transactions hence the adversaries who intentionally harm the mission and selfish members due to lack of resources can be identified and isolated from the network by the way authentication can be achieved and secure group can be formed.

Trust and Cluster based Security Architecture (TCS)

This model could ensure the authentication, by identifying untrusted soldiers and also addresses the scalability issue. Here, authentication is ensured by evaluating trustworthiness of soldiers based on direct observations and feedback values. Based on these two values, overall trust is calculated then by using the overall trust, cluster is formed.

Trust based Authentication Scheme.

In this model, in order to evaluate the trustworthiness of participating nodes, direct observation and feedback values is used. Based on these two values, aggregated trust is calculated then untrusted nodes could be identified and eliminated from the network.

5. Conclusion

MANET is a suitable network for applications where infrastructure is not possible or needs to be deployed on demand. The significant nature such as lack of central administration, open and shared wireless medium, nodes as routers, no fixed topology, self-organize and other characteristics of MANET offer various applications. Among the applications, military environment is getting more attention due to the necessity and adaptability of MANET in such environment.

The objective of MANET based military environment is to provide continuous access to all soldiers and decision makers to form a clear and perfect view of the military environment so

that it leads to successful completion of mission by making use of network functionalities. But achieving it, is not an easy task due to the unique characteristics of MANET.

Routing of information from one place to another place in MANET based military environment is achieved by routing protocols. Routing protocols are designed in nature to support network operations. But in practice, they are affected by security vulnerabilities in the form of various attacks. Black hole attack is one of the dangerous attacks because it is launched internally by compromised nodes and also originates to disturb the network operation in the routing stage itself. Hence providing secure routing is a challenging task.

In addition, authentication is an important security requirement because it provides first level of security among the security requirements. However, providing authentication is a difficult task since each soldier has to communicate with other soldiers in the unstable environment without any prior interactions and recommendations. This loophole, leads security vulnerabilities in MANET.

However, authentication is ensuring the right identity but it does not guarantee the trusted route from the source to destination because routing operations are still affected by compromised or selfish nodes. They may ensure authentication but not cooperation in routing operations.

To safeguard the network from the above issues several solutions were proposed but they are based on cryptographic techniques such as Shared Secret, Public Key Infrastructure (PKI), Digital Signature, Digital Certificate and Hash functions. These techniques are centralized, pre-determined, depend on trusted third party consequently increasing computation power, memory, consumption of communication bandwidth and battery power leading to performance degradation in network's throughput, availability and robustness as MANET has resource constrained nodes. In addition, the above techniques are inefficient to handle internal attacks.

To overcome the above shortcomings and lack of integration trust based solutions such as detection of black hole attack, ensuring authentication and trusted route formation, are the foundation of this research work. Consequently, the trust based security models are proposed.

UNIVERSITY GRANTS COMMISSION
BAHADUR SHAH ZAFAR MARG
NEW DELHI – 110 002

STATEMENT OF EXPENDITURE IN RESPECT OF MAJOR RESEARCH PROJECT

1. Name of Principal Investigator : **Dr. S. SIVAGURUNATHAN**

2. Deptt. of Principal Investigator : **Department of Computer Science and Applications**

   University/College : **The Gandhigram Rural Institute – Deemed to be University, Gandhigram.**

3. UGC approval Letter No. and Date : **F. No. 42-128/2013 (SR)**, Dated: **14-03-2013**.

4. Title of the Research Project : **Trust Based Authentication Mechanism for Mobile Ad-Hoc Network**

5. Effective date of starting the project : **01-04-2013**

6. a. Period of Expenditure: **From 01-04-2013 To 31-03-2017**

   b. Details of Expenditure:

S. No.	Item	Amount Approved (Rs.)	Expenditure Incurred (Rs)	Excess/ Re-appropriation/diff.
i.	Books & Journals	80,000.00	77,746.00	2,254.00
ii.	Equipment	1,50,000.00	1,44,945.00	5,055.00
iii.	Contingency	67,500.00	94,292.00	-26,792.00*
iv.	Field Work/Travel (Give details in the proforma at Annexure-IV).	45.000.00	40,909.00	4,091.00
v.	Hiring Services	40,500.00	42,000.00	-1,500.00*
vi.	Special Need	75,000.00	--	75,000.00
vii.	Overhead	27,000.00	27,000.00	--
viii.	Any other items (Please specify)	--	--	--
	Total	**4,85,000.00**	**4,26,892.00**	**58,108.00**

* Re-appropriate 20% of fund allotted under the special need into Hiring services and contingency head.

c . Staff : - **Not Applicable**

Date of Appointment: --

S.No	Items	From	To	Amount Approved (Rs.)	Expenditure incurred (Rs.)
1.	Honorarium to PI (Retired Teachers) @ Rs. 18,000/-p.m.				
2.	**Project fellow:** i) **NET/GATE qualified**-Rs. 16,000/- p.m. for initial 2 years and Rs. 18,000/- p.m. for the third year. ii) **Non-GATE/Non-NET**- Rs. 14,000/- p.m. for initial 2 years and Rs. 16,000/- p.m. for the third year.				

1. It is certified that the appointment(s) have been made in accordance with the terms and conditions laid down by the Commission.

2. If as a result of check or audit objection some irregularly is noticed at later date, action will be taken to refund, adjust or regularize the objected amounts.

3. Payment @ revised rates shall be made with arrears on the availability of additional funds.

4. It is certified that the grant of **Rs. 4,85,000/=** (Rupees Four Lakhs Eighty Five thousand only) received from the University Grants Commission under the scheme of support for Major Research Project entitled **"Trust Based Authentication Mechanism for Mobile Ad-Hoc Network"** vide UGC letter No. **F. 42-128/2013 (SR)** dated **14-03-2013** has been fully utilized for the purpose for which it was sanctioned and in accordance with the terms and conditions laid down by the University Grants Commission.

SIGNATURE OF THE PRINCIPAL INVESTIGATOR

Dr. S. SIVAGURUNATHAN
PRINCIPAL INVESTIGATOR
UGC-MAJOR RESEARCH PROJECT
F.No: 42-128/2013 (SR)
GANDHIGRAM RURAL INSTITUTE-DEEMED UNIVERSITY
GANDHIGRAM-624 302, TAMILNADU, INDIA

REGISTRAR

REGISTRAR
Gandhigram Rural Institute

STATUTORY AUDITOR

For S.S. & Co
Chartered Accountants

S.Srinivasan Partner
FRN:003502S(Mem.No:024142)

S.S. & Co B-9, 2nd Floor, Seetha Apts. Madurai 625 002 Chartered Accountants

UNIVERSITY GRANTS COMMISSION
BAHADUR SHAH ZAFAR MARG
NEW DELHI – 110 002

STATEMENT OF EXPENDITURE INCURRED ON FIELD WORK

Name of the Principal Investigator: **Dr. S. Sivagurunathan**

Name of the Place visited	Duration of the Visit		Mode of Journey	Expenditure Incurred (Rs.)
	From	To		
UGC, New Delhi	21-12-2014	25-12-2014	Air/Taxi	40,909.00
			Total	**40,909.00**

Certified that the above expenditure is in accordance with the UGC norms for Major Research Projects.

SIGNATURE OF THE PRINCIPAL INVESTIGATOR

Dr. S. SIVAGURUNATHAN
PRINCIPAL INVESTIGATOR
UGC-MAJOR RESEARCH PROJECT
F.No: 42-128/2013 (SR)
GANDHIGRAM RURAL INSTITUTE-DEEMED UNIVERSITY
GANDHIGRAM-624 302, TAMILNADU, INDIA

REGISTRAR

12/10/15

REGISTRAR
Gandhigram Rural Institute

STATUTORY AUDITOR

For S.S. & Co.
Chartered Accountants

Srinivasan Partner
[redacted]3502 S (Mem.No:024142)

S.S. & Co
B-9, 2nd Floor, Seetha Apts, Madurai 625 002
Chartered Accountants

Final Report Assessment / Evaluation Certificate

(Two Members Expert Committee Not Belonging to the Institute of Principal Investigator)

(to be submitted with the final report)

It is certified that the final report of Major Research Project entitled " **Trust Based Authentication Mechanism for Mobile Ad-Hoc Network"** by **Dr. S. Sivagurunathan**, Department of Computer Science and Applications, The Gandhigram Rural Institute - Deemed to be University, Gandhigram has been assessed by the committee consisting the following members for final submission of the report to the UGC, New Delhi under the scheme of Major Research Project (**F.No.:42-128/2013(SR), dated: 14-03-2013**).

Comments/Suggestions of the Expert Committee:-

- The Objectives mentioned in the Research proposal entitled "Trust Based Authentication Mechanism for Mobile Ad-Hoc Network" were completed satisfactorily.
- The obtained results have been published in peer reviewed International Journals.
- Overall, the outcome of the Research Project is Very Good.
- The Report has been prepared as per the guidelines.

Name & Signatures of Experts with Date:-

S. No.	Name of Expert	University/College name	Signature with Date
1.	Dr. E. Sivasankar,	Department of Computer Science and Engineering, National Institute of Technology, Tiruchirapalli – 620 015	6/12/2018 ASSISTANT PROFESSOR Dept. of Computer Sci. & Engg. National Institute of Technology, TIRUCHIRAPPALLI - 620 015, INDIA
2.	Dr. S. Parthasarathy	Department of Computer Applications, Thiagarajar College of Engineering, Madurai – 625 015	17/12/2018 Dr.S.Parthasarathy Head of the Dept. Dept. Of Computer Applications Thiagarajar College of Engineering Madurai - 625 015

It is certified that the final report has been uploaded on UGC-MRP portal on ..... .

It is also certified that final report, Executive summary of the report, Research documents, monograph academic papers provided under Major Research Project have been posted on the website of the University/College.

REGISTRAR

Annexure - VIII

UNIVERSITY GRANTS COMMISSION
UTILIZATION CERTIFICATE – From 16.04.2013 to 31.03.2017

It is certified that the amount of **Rs.4,26,892/-** (Rupees Four lakhs twenty-six thousand eight hundred and ninety-two only) out of the grant of **Rs.4,85,000**/-(Rupees Four lakhs eighty-five thousand only) Sanctioned to Dr.S.Sivagurunathan, Assistant Professor and PI, Department of Computer Science and Applications by the University Grants Commission vide its letter No.42-128/2013/(SR),dated.14.03.2013 towards UGC-MRP on **" Trust based authentication mechanism for mobile ad hoc network"** under UGC-MRP scheme has been utilized for the purpose for which it was sanctioned and in accordance with the terms and conditions as laid down by the commission.

If as a result of check or audit objection some irregularities are noticed at a later stage, action will be taken for refund, adjustment or regulation.

Signature
Registrar / Principal with seal 13/10/17
REGISTRAR
Gandhigram Rural Institute

Signature
Finance Officer with seal
Special Officer (Finance)
Gandhigram Rural Institute

Signature
Principal Investigator with seal

Dr. S. SIVAGURUNATHAN
PRINCIPAL INVESTIGATOR
UGC-MAJOR RESEARCH PROJECT
F.No: 42-128/2013 (SR)
GANDHIGRAM RURAL INSTITUTE-DEEMED UNIVERSITY
GANDHIGRAM-624 302, TAMILNADU, INDIA

For A.V. SUBRAMANIAN & CO.
CHARTERED ACCOUNTANTS

Signature, Chartered Accountant
with seal and Registrar No. C.A. J. Sumathi
M. No: 029617, Partner
ICAI FRN: 010154S
(If the accounts were audited prior to the audit of Statutory Auditors)

Note: The University/ Institution will submit an audited statement of accounts, duly audited by the Statutory Auditors of the University / Institution as soon as the accounts of the University / Institution are audited.

Annexure - VII

The Gandhigram Rural Institute – Deemed University
Gandhigram - 624 302
UGC-MRP Project on "Trust based authentication mechanism for mobile ad hoc network"
Dr.S.Sivagurunathan, Assistant Professor, Dept.of computer Science and Applications

University/Institution : The Gandhigram Rural Institute-Deemed University, Gandhigram-624 302
Sanction Letter No. and Date of UGC, New Delhi : F.42-128/2013/(SR),dt: 14.03.2013
Statement of Actual Expenditure during : 16.04.2013 to 31.03.2017

Item of Expenditure	Total Grant approved	Actual Grant Received				Total (3 to 6)	Actual Expenditure incurred				Total (8 to 11)	Excess/Saving diff. of Co.7 & 12
1	2	3	4	5	6	7	8	9	10	11	12	13
		2013-14	2014-15	2015-16	2016-17		2013-14	2014-15	2015-16	2016-17		
(A) Non-Recurring												
1. Equipment	1,50,000	1,50,000	-	-	-	1,50,000	1,09,250	0	35,695	-	1,44,945	5,055
2. Books and Journals	80,000	80,000	-	-	-	80,000	6,257	71,489	-	-	77,746	2,254
Total (A)	**2,30,000**	**2,30,000**	-	-	-	**2,30,000**	**1,15,507**	**71,489**	**35,695**	**0**	**2,22,691**	**7,309**
(B) Recurring (Per Annum)												
1.Project Fellow - 2 Years	0	0	-	-	-	0	0	0	0	0	0	0
2.Chemical/Glasswar e/Conumable	0	0	-	-	-	0	0	0	0	0	0	0
2.Hiring Services	45,000	22,500	-	-	18,000	40,500	0	42,000	0	0	42,000	-1,500
3.Contingencies	75,000	37,500	-	-	30,000	67,500	3,437	24,740	29,414	36,701	94,292	-26,792
4.Travel/Field Work	50,000	25,000	-	-	20,000	45,000	0	40,909	0	0	40,909	4,091
5.Special Need	1,50,000	75,000		-	-	75,000	0	0	0	0	0	75,000
5.Overhead Charges	27,000	27,000	-	-	-	27,000	0	27,000	0	0	27,000	0
Total (B)	**3,47,000**	**1,87,000**	-	-	**68,000**	**2,55,000**	**3,437**	**1,34,649**	**29,414**	**36,701**	**2,04,201**	**50,799**
Total (A) + (B)	**5,77,000**	**4,17,000**	-	**0**	**68,000**	**4,85,000**	**1,18,944**	**2,06,138**	**65,109**	**36,701**	**4,26,892**	**58,108**
Interset on Grant received		12,310	10,598	3,834	2,066	28,808		**0**	**0**	**0**	0	28,808
Total	**5,77,000**	**4,29,310**	**10,598**	**3,834**	**70,066**	**5,13,808**	**1,18,944**	**2,06,138**	**65,109**	**36,701**	**4,26,892**	**86,916**
Unspent Balance												**86,916**

Total Grant received with interest	**5,13,808**
Less: Expenditure	**4,26,892**
Unspent Balance as on 31.03.2017	**86,916**

Certified that the grant has been utilized for the purpose for which if was sanctioned and in accordence with terms and conditions attached to

Dr. S. SIVAGURUNATHAN
PRINCIPAL INVESTIGATOR
UGC-MAJOR RESEARCH PROJECT
F.No: 42-128/2013 (SR)
GANDHIGRAM RURAL INSTITUTE-DEEMED UNIVERSITY

Special Officer (Finance)
Gandhigram Rural Institute

V. S. Sivagurunathan 13/10/17
REGISTRAR
Gandhigram Rural Institute

For A.V. SUBRAMANIAN & CO,
CHARTERED ACCOUNTANTS
C.A. J. Sumathi
M. No: 029617, Partner
ICAI: FRN: 010643S