Trust Enhanced Security Framework for Mobile Ad hoc Wireless Networks

By

Venkatesan Balakrishnan

A thesis submitted to Macquarie University

for the degree of

Doctor of Philosophy

Department of Computing

November 2010

Typeset in LaTeX 2_ε.

Except where acknowledged in the customary manner, the material presented in this thesis is, to the best of my knowledge, original and has not been submitted in whole or part for a degree in any university.

Venkatesan Balakrishnan

Acknowledgements

I am very thankful to *Prof. Vijayaraghavan Varadharajan*, without whom I would have never reached to this stage of my professional career. I am grateful to him for his guidance and also his motivational talks during those hard moments. I thank him for sharing his knowledge and vision on a variety of thought-provoking topics, ranging from technical to philosophical that have added a new dimension to my thought process. I would like to express my gratitude to *Dr. Udaya Tupakula*, who provided valuable technical insights into my research work and, therefore been a significant factor for its progression. I dedicate all my publications to him, especially to his efforts in reviewing all the draft versions and constantly emerging out with suggestions for improvements, until those drafts were published. I appreciate *Ms. Andrina Brennan* for her kindness and the difference she made to my research work by saving innumerable hours that would have been lost in administration works. I would like to thank *Defence Signals Directorate (DSD), Australia* for supporting this research work.

I am thankful to *Dr. Sarath Indrakanti*, who inspired me with his research dedication and for sharing his research experience and working with me during those countless long nights. I would like to thank *Dr. Vijayakrishnan Pasupathinathan* for his stimulating technical discussions and being there whenever I invited him for a short-break from research work. My research implementation would have not met the deadlines without the contributions from *Phillip Lucs*. I am very grateful to him for bringing many years of his industrial experience in software engineering and, working countless nights and weekends with me during his Bachelors Honours degree. I am very thankful

to *Dr. Venkatakrishnan Balasubramanian Appiah* for his motivational speeches on various topics and helping me to get the casual academic teaching role that supported my financial requirements. I thank *Dilshan Jayarathna*, *Adam Shah*, *Suresh Mulavineth* and *Richard Miller* for providing the technical resources and supplying with Gigabytes of storage space for my simulation logs, in particular, during those days when Gigabytes of storage space was expensive. I appreciate *Dr. Marie Elisabeth Gaup Moe* from NUST, Norway for sharing her knowledge on MANETs that support anonymous communications. *Mark Bazant*, who was my Team Lead at CSC deserves a loud appreciation for accommodating my leave and time-in-lieu requests without which the thesis writing would have been further delayed. I am thankful to the thesis proof-reader, *Tony Roberts* for his quick responses, regardless of the time of the day or night and, polishing this thesis within a short notice. I would also like to thank the thesis reviewers for their time and effort in reviewing this thesis and providing valuable comments and feedbacks.

To all the well-wishers, who have supported me all these years. Foremost thanks goes to *Rajesh Udayamurthy* and *Ramya Rajesh* for being kind, supportive and caring to me during those solitary days of my research degree. My ex-flatmate, *Jayachandra Rao* stands out among all the hearts that enabled me to transform a research idea into this well-researched thesis work. I am very grateful for his generosity that took care of all house-keeping activities and provided cooked food regardless of the time of the day or night. I dedicate this thesis to him for his selfless nature and all the care that he has showered during my stay with him. I am very grateful and thankful to my mentors, *Dr. Archana Parashar* and *Dr. M Vasudevacharya* for their support, love and guidance for all these years, without which none of the significant accomplishments and progressions would have happened during the last eight years of my life. To my loveable parents and adorable brothers, who have been wonderful, selfless and been a platform to make all my dreams come true. And to my admirable wife, who is always there for me. Finally, to the fundamental physical forces in this universe that manifested this insignificant agglomeration of atoms and molecules to reach a significant achievement during its lifetime.

List of Publications

Book Chapters

- V. Balakrishnan, V. Varadharajan, and U. K. Tupakula, *Trust Management in Mobile Ad hoc Networks*. Handbook of Wireless Ad hoc and Sensor Networks, Springer (London), 2009.

- V. Balakrishnan, V. Varadharajan, and U. K. Tupakula, *Security and Authentication*. Mobile Wireless Networks: Integrated Service Issues, Wiley-Blackwell, 2009.

- V. Balakrishnan, V. Varadharajan, U. K. Tupakula, and P. Lucs, *SMRTI:: Secure MANET Routing with Trust Intrigue*. Mobile Intelligence: Mobile Computing and Computational Intelligence, John Willey & Sons, Inc., 2010.

- V. Balakrishnan, V. Varadharajan, and U. K. Tupakula, *Security in Mobile Ad-hoc Networks*. Handbook of Communication Networks and Distributed Systems, World Scientific (Singapore) (*Accepted for publication*).

Conference Proceedings

- V. Balakrishnan, V. Varadharajan, and U. K. Tupakula, *Subjective Logic Based Trust Model for Mobile Ad-hoc Networks*. Proceedings of the 4^{th} ACM International Conference on Security and Privacy in Communication Networks (SecureComm 2008), Istanbul, Turkey, September 2008.

- V. Balakrishnan, V. Varadharajan, U. K. Tupakula, and P. Lucs, *TEAM: Trust Enhanced Security Architecture for Mobile Ad-hoc Networks*. Proceedings of the 15^{th} IEEE International Conference on Networks (ICON 2007), Adelaide, Australia, pp. 182-187, November 2007.

- V. Balakrishnan, V. Varadharajan, U. K. Tupakula, and P. Lucs, *Trust Integrated Cooperation Architecture for Mobile Ad-hoc Networks*. Proceedings of the 4^{th} IEEE International Symposium on Wireless Communication Systems (ISWCS 2007), Trondheim, Norway, pp. 592-596, October 2007.

- V. Balakrishnan, V. Varadharajan, U. K. Tupakula, and M. E. Gaup Moe, *Mitigating Flooding Attacks in Mobile Ad-hoc Networks Supporting Anonymous Communications*. Proceedings of the 2^{nd} IEEE International Conference on Wireless Broadband and Ultra Wideband Communication (AusWireless 2007), Sydney, Australia, pp. 29-34, August 2007.

- V. Balakrishnan, V. Varadharajan, U. K. Tupakula, and P. Lucs, *Trust and Recommendations in Mobile Ad hoc Networks*. Proceedings of the 3^{rd} International Conference on Networking and Services (ICNS 2007), Athens, Greece, pp. 64-69, June 2007.

- V. Balakrishnan, V. Varadharajan, P. Lucs, and U. K. Tupakula, *Trust Enhanced Secure Mobile Ad hoc Network Routing*. Second IEEE International Symposium on Pervasive Computing and Ad Hoc Communications (PCAC 2007), Proceedings of the 21^{st} IEEE International Conference on Advanced Information Networking and Applications Workshops(AINAW 2007), Niagara Falls, Canada, pp. 27-33, May 2007.

- V. Balakrishnan, V. Varadharajan, and U. K. Tupakula, *Fellowship: Defense against Flooding and Packet Drop Attacks in MANET*. Proceedings of the 10^{th} IEEE/IFIP Network Operations and Management Symposium (NOMS 2006), Vancouver, Canada, pp. 1-4, April 2006.

- V. Balakrishnan, and V. Varadharajan, *Fellowship in Mobile Ad hoc Networks*. Proceedings of the 1^{st} IEEE International Conference on Security and Privacy in Communications Networks (SecureComm 2005), Athens, Greece, pp. 225-227, September 2005.

- V. Balakrishnan, and V. Varadharajan, *Packet Drop Attack: A Serious Threat to Operational Mobile Ad hoc Networks*. Proceedings of the International Conference on Networks and Communication Systems (NCS 2005), Krabi, Thailand, pp. 89-95, April 2005.

- V. Balakrishnan, and V. Varadharajan, *Designing Secure Wireless Mobile Ad hoc Networks*. Proceedings of the 19^{th} IEEE International Conference on Advanced Information Networking and Applications (AINA 2005), Taipei, Taiwan, pp. 5-8, March 2005.

Abstract

The advent of wireless communication and the proliferation of handheld devices have significantly advanced the growth of nomadic communications. Capability of these handheld mobile devices to self-organise themselves on fly in the absence of an infrastructure and to extend their communications beyond their wireless radio range have potentially led to the development of Mobile Ad hoc Networks (MANET). Security is one of the most indispensable research areas and plays a central role in determining the success of civilian and commercial mobile ad hoc networks. Unfortunately, mobile nodes struggle to enlist trusted intermediaries for communication with various destinations since trusted intermediaries are a prerequisite to keep those communications alive and free from active attacks. Although few integrated security systems exist for the MANETs, a two-layered (prevention and detection-reaction systems) trust-enhanced security architecture is yet to be seen for the MANETs to the best of our knowledge. The two-layered approach is so required for the prevention and detection-reaction systems to complement each other to deliver a trustworthy, secure, and an operational routing layer amidst the inherent issues.

Therefore this thesis, (a) *focuses on the systematic study of the security threats and attacks and, adversaries in the MANETs and accordingly the analysis of the strength of solutions that have been proposed within different categories of security systems*, (b) *proposes novel techniques to meet the shortcomings of proposed security solutions and thence to develop a realistic two-layered* ***Trust Enhanced security Architecture***

for the MANETs (TEAM). These novel techniques include, (a) *an obligation-based* ***fellowship*** *model to motivate cooperation among the mobile nodes*, (b) ***Secure MANET Routing with Trust Intrigue (SMRTI)*** *that resolves the limitations harboured by related trust models and capitalises all the evidence that are available within the limitations of the MANET for making better routing decisions* and, (c) *a new secure routing protocol known as* ***Scasec***. Furthermore, fellowship model is extended to defend flooding attacks in the MANETs that support anonymous communications. Similarly, SMRTI is extended to incorporate subjective logic with a focus to resolve the notion of uncertainty in the trust relationships established between newly-joining and existing mobile nodes. Finally, the better performance results of all these proposed techniques are demonstrated using varied simulation scenarios.

Contents

List of Figures

List of Tables

Listings

List of Acronyms

The following list of acronyms is neither exhaustive nor exclusive, but presents the key acronyms used in this thesis.

ACK ..... *Ack*nowledgement

ANODR ..... *An*onymous *O*n-*d*emand *R*outing

AODV ..... *A*d-hoc *O*n-demand *D*istance *V*ector

ARAN ..... *A*uthenticated *R*outing for *A*d-hoc *N*etworks

ARM ..... *A*nonymous *R*outing Protocol for *M*ANET

ARP ..... *A*ddress *R*esolution *P*rotocol

ASR ..... *A*nonymous *S*ecure *R*outing

BISS ..... *B*uilding Secure Routing out of an *I*ncomplete *S*et of *S*ecurity Association

CA ..... *C*entralised *A*uthority

CAR ..... *C*hain-based *A*nonymous *R*outing

CBR ..... *C*onstant *B*it *R*ate

CCS ..... *C*redit *C*learance *S*ervice

CONFIDANT *C*ooperation *o*f *N*odes: *F*airness *i*n *D*ynamic *A*d-hoc *Net*works

CREQ ..... *C*ertificate *Req*uest

CTS ..... *C*lear *t*o *S*end

DCF ..... *D*istributed *C*oordination *F*unction

DoS ..... *D*enial *o*f *S*ervice

DSR ..... *D*ynamic *S*ource *R*outing

DSSS ..... *D*irect *S*equence *S*pread *S*pectrum

FIFO ..... *F*irst *i*n *F*irst *o*ut

HMAC ..... *M*essage *A*uthentication *C*ode

IDS ..... *I*ntrusion *D*etection *S*ystem

IFQ ..... *I*nter*f*ace *Q*ueue

MAC ..... *M*edium *A*ccess Layer

MANET ..... *M*obile *A*d hoc *Net*works

MOCA ..... *Mo*bile *CA*

NAV ..... *N*etwork *A*llocation *V*ector

NS2 ..... *N*etwork *S*imulator *2*

PDA ..... *P*ersonal *D*igital *A*ssistant

PDR ..... *P*acket *D*elivery *R*atio

PGP ..... *P*retty *G*ood *P*rivacy

PKG ..... *P*ublic *K*ey *G*enerator

PPM ..... *P*acket *P*urse *M*odel

PTM ..... *P*acket *T*rade *M*odel

QoS ..... *Q*uality *o*f *S*ervice

RERR ..... *R*oute *Err*or

RREP ..... *R*oute *Rep*ly

RREQ ..... *R*oute *Req*uest

RTS ..... *R*equest *t*o *S*end

SAODV ..... *S*ecure *A*d-hoc *O*n-demand *D*istance *V*ector

SCASEC ..... *Sca*lable Multi-service Group Key based *Sec*ure Routing Protocol

SEKM ..... *S*ecure and *E*fficient *K*ey *M*anagement

SL-SMRTI .... *S*ubjective *L*ogic based *SMRTI*

SMG ..... *S*calable *M*ulti-service *G*roup Key Management

SMRTI ..... *S*ecure *M*ANET *R*outing with *T*rust *I*ntrigue

SRD ..... *S*uccessful *R*oute *D*iscovery

SRP ..... *S*ecure *R*outing *P*rotocol

TEAM ..... *T*rust *E*nhanced Security *A*rchitecture for *M*ANET

TORA ..... *T*emporally-*O*rdered *R*outing *A*lgorithm

TRR ..... *T*rust *R*ecomendation *R*equest

TTL ..... *T*ime *t*o *L*ive

UML ..... *U*nified *M*odeling *L*anguage

VANET ..... *V*ehicular *A*d hoc *Net*works

List of Symbols

The following list of symbols is neither exhaustive nor exclusive, but highlights the symbols used in our models for the sake of completeness.

M ..... Notation for a message

T ..... Notation for trust metric

P ..... Set of positive evidence

N ..... Set of negative evidence

R ..... Representation of a route

x ..... Notation for a preposition

f ..... Notation for communication flow

p ..... Total number of positive evidence

n ..... Total number of mobile nodes (elsewhere)
Total number of negative evidence (Chapter 9)

E ..... Set of events (route request, route reply, route error, *etc.*)

l ..... Cardinality of sensitivity levels (elsewhere)
Interval count for which recommendation is absent (Chapter 9)

k ..... Interval count for which mobile nodes are out of communication

$\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ ..... Representation of mobile nodes

K(A) ..... Notation for data keying matrix

S(A) ..... Matrix for managing the communication groups

RR ..... Representation of, direct, observed, or recommended reputation

Bandwidth(A) .. Physical channel bandwidth of $\mathcal{A}$

pos(event) ..... Positive value for a benign behaviour

neg(event,action) Negative value for a malicious action

$p^{\mathcal{A}}, q^{\mathcal{A}}$ ..... Large primes of $\mathcal{A}$

P_k ..... Notation for a packet k

$K_{\mathcal{S}-session}$ ..... Session key generated by $\mathcal{S}$

r_1, r_2, r_3 ..... Notation for a sensitivity levels

$K_{\mathcal{SD}}$ ..... Shared secret between $\mathcal{S}$ and $\mathcal{D}$

$s^{\mathcal{A}}$ ..... Notation for $\mathcal{A}$'s master secret key

$T_{\mathcal{I}}, U_{\mathcal{I}}$ ..... Random numbers generated by $\mathcal{I}$

t_0 ..... Network deployment time period

R_0 ..... Notation for the initial reputation

V_{max} ..... Maximum velocity of a mobile node

$C_{\mathcal{A}-Contribution}$ .. $\mathcal{A}$'s battery energy for other nodes

$C_{\mathcal{A}-Self}$ ..... $\mathcal{A}$'s battery energy for self operations

$PK_{\mathcal{I}}$ ..... One-time public key generated by $\mathcal{I}$

$n_{\mathcal{I}}$ ..... All nodes in the network excluding $\mathcal{I}$

$\mathbb{R}_{\mathcal{I}}$ ..... Set of trust relationships held between $\mathcal{I}$ and $n_{\mathcal{I}}$

$\mathbb{R}_{\mathcal{IJ}}$ ..... Represents the trust relationship between $\mathcal{I}$ and $\mathcal{J}$

S_i ..... A segment within the reputation range $[-1, +1]$

CG_1, CG_2, CG_3 Communication groups based on sensitivity level

a_x ..... Base rate that optimistically views uncertainty as belief for x

u_x ..... Belief that is neither committed to the truth nor falsehood of x

$HMAC_{SK^{\mathcal{S}}}(M)$ HMAC of M using $SK^{\mathcal{S}}$

$K_{\mathcal{SD}}(M)$ ..... Encryption of M using $K_{\mathcal{SD}}$

$\{M\}_{PK_{\mathcal{I}}}$ ..... Encryption of M using $PK_{\mathcal{I}}$

$E_{\mathcal{A}}(t_0)$ ..... Battery energy of $\mathcal{A}$ at t_0

$E_{\mathcal{A}}(P_k)$ ..... $\mathcal{A}$'s battery energy to transmit P_k

$H_1(\mathcal{I})$ ..... Notation for a one-way function

$T_{\mathcal{I}}Flow_f(t_{a+1})$.. $\mathcal{I}$'s trustworthiness for f at $t_{(a+1)}$

$T_{\mathcal{I}}Route_R(t_{a+1})$. $\mathcal{I}$'s trustworthiness for R at $t_{(a+1)}$

$T_{\mathcal{I}}Node_{Src}(t_a)$.. $\mathcal{I}$'s trustworthiness for node Src at t_a

$E(\omega_x)$ ..... Probability expectation value of an opinion

$P_{pub}^{\mathcal{A}}$ ..... Notation for $\mathcal{A}$'s public key

$\mathbb{G}_1^{\mathcal{A}}$ ..... Notation for $\mathcal{A}$'s additive group

$\mathbb{G}_2^{\mathcal{A}}$ ..... Notation for $\mathcal{A}$'s multiplicative group

$S_{\mathcal{I}}^{\mathcal{A}}$ ..... Notation for $\mathcal{A}$'s participant key to $\mathcal{I}$

$CG_k^{\mathcal{A}}$ ..... Notation for $\mathcal{A}$'s CG_k with sensitivity level k

$S_{\mathcal{M}k}^{\mathcal{A}}$ ..... Denotes whether or not $\mathcal{A}$ considers $\mathcal{M}$ for $CG_k^{\mathcal{A}}$

$SK_k^{\mathcal{A}}$ ..... $\mathcal{A}$'s session secret key for f that belongs to $CG_k^{\mathcal{A}}$

$Auth_k^{\mathcal{A}}$ ..... $\mathcal{A}$'s authorisation for nodes that belong to $CG_k^{\mathcal{A}}$

$\oslash$ ..... Fading operator

$\oplus$ ..... Consensus operator

$\otimes$ ..... Discounting operator

$\geqslant$ ..... Comparison operator

θ ..... Length of S_i

σ ..... Merit factor

λ ..... Demerit factor

Δ ..... Threshold-limit

η ..... Contribution-share

χ ..... Contribution-common

μ ..... Redemption threshold

ρ ..... Negotiation threshold

ν ..... Transmission threshold

Θ ..... Frame of discernment

α, β ..... Beta PDF parameters

ϕ ..... Count of new neighbours

γ ..... Relative weight (Chapter 9)
Packet forwarding ratio (elsewhere)

δ ..... Reputation decay (or) growth factor

∇ ..... Evidence-to-opinion mapping operator

τ ..... Reception threshold (elsewhere)
Average duration taken for f (Chapter 9)

Ω ..... Set of opinions (direct, observed and recommended)

σ ..... Contains timestamps of opinion initialisation or last revision

δ_n ..... Name of a cluster

b_x ..... Belief that x is true

d_x ..... Disbelief that x is false

Δ_c ..... Threshold-limit for a context

Δ_r ..... Threshold-limit for derived recommendations

$\beta_{\mathcal{J}}$ ..... $\mathcal{J}$'s weight in the route during trust evaluation

ω_x ..... Binomial subjective opinion about the truth of x

δ_t ..... Represents the type of relationship in a cluster-based MANET

${}^{\mathcal{A}}\eta_{\mathcal{I}}$ ..... $\mathcal{A}$'s contribution-share for $\mathcal{I}$

${}^{\mathcal{A}}\tau_{\mathcal{I}}$ ..... $\mathcal{A}$'s reception threshold for $\mathcal{I}$

${}^{\mathcal{A}}T_{\mathcal{I}}$ ..... $\mathcal{A}$'s blacklist timestamp for $\mathcal{I}$

$^{\mathcal{I}}\tau_{\mathcal{A}}^{recp}$ ..... $\mathcal{I}$'s reciprocate reception for $\mathcal{A}$

$^{\mathcal{A}}\nu_{\mathcal{J}}$ ..... $\mathcal{A}$'s transmission threshold for $\mathcal{J}$

$^{\mathcal{A}}\gamma_{\mathcal{J}}$ ..... $\mathcal{A}$'s packet forwarding ratio for $\mathcal{J}$

$^{\mathcal{A}}\beta_{\mathcal{J}}$ ..... Total count of packets transmitted to $\mathcal{J}$ by $\mathcal{A}$

$^{\mathcal{A}}\alpha_{\mathcal{J}}$ ..... Total count of packets forwarded by $\mathcal{J}$ on behalf of $\mathcal{A}$

$^{\mathcal{A}}\omega_{\mathcal{B}}^{m}$ ..... $\mathcal{A}$'s opinion (of type m) on $\mathcal{B}$

$^{\mathcal{A}}b_{\mathcal{B}}^{m}$ ..... $\mathcal{A}$'s belief (with respect to m) on $\mathcal{B}$

$^{\mathcal{A}}d_{\mathcal{B}}^{m}$ ..... $\mathcal{A}$'s disbelief (with respect to m) on $\mathcal{B}$

$^{\mathcal{A}}u_{\mathcal{B}}^{m}$ ..... $\mathcal{A}$'s ignorance (with respect to m) on $\mathcal{B}$

$\omega_x^{\mathcal{A}}$ or $\omega(\mathcal{A}:x)$. $\mathcal{A}$'s opinion on x

$\omega_x^{\mathcal{R}:\mathcal{S}}$ ..... $\omega_{\mathcal{S}}^{\mathcal{R}}$ discounts $\omega_x^{\mathcal{S}}$

$\omega_x^{\mathcal{P}\diamond\mathcal{Q}}$ ..... Consensus opinion of $\omega_x^{\mathcal{P}}$ and $\omega_x^{\mathcal{Q}}$

$\omega_{\mathcal{I}\mathcal{J}}^{RR}(t_a)$ ..... $\mathcal{I}$'s reputation of type RR for $\mathcal{J}$ at t_a

$\omega_{\mathcal{I}\mathcal{J}}^{Direct}(t_a)$ ..... $\mathcal{I}$'s accrued direct reputation for $\mathcal{J}$ at t_a

$\omega_{\mathcal{I}\mathcal{J}}^{Observed}(t_a)$ .... $\mathcal{I}$'s accrued observed reputation for $\mathcal{J}$ at t_a

$\omega_{\mathcal{I}\mathcal{J}}^{Rec}(t_a)$ ..... $\mathcal{I}$'s accrued recommended reputation for $\mathcal{J}$ at t_a

$\gamma_{\mathcal{I}\mathcal{J}}^{RR}$ ..... $\mathcal{R}\mathcal{R}$'s weight in the trust evaluation of $\mathcal{I}$ for $\mathcal{J}$