AUTHENTICATION FOR MULTI-LOCATED PARTIES AND WIRELESS AD HOC NETWORKS

By

PRADEEP KUMAR DANTALA

Bachelor of Technology in Computer Science & Engineering
Jawaharlal Nehru Technological University
Hyderabad, Andhra Pradesh
2009

Submitted to the Faculty of the
Graduate College of the
Oklahoma State University
in partial fulfillment of
the requirements for
the Degree of
MASTER OF SCIENCE
July, 2011

AUTHENTICATION FOR MULTI-LOCATED

PARTIES AND WIRELESS AD HOC NETWORKS

Thesis Approved:

Dr. Subhash Kak

Thesis Adviser

Dr. Johnson Thomas

Dr. David Cline

Dr. Mark E. Payton

Dean of the Graduate College

ACKNOWLEDGMENTS

I would like to thank Dr.Subhash Kak for his guidance and supervision he has given me during the entire span of this research work and my thesis. I feel extremely privileged to be a part of his research team and would like to extend my deepest gratitude for bringing out the best in me and helping me channelize my efforts in the right directions. He always motivated me to achieve my goals with steadfast dedication and continually encouraged to move forward inspite of witnessing initial failures. New ideas were always discussed and his timely advice has helped me a lot to explore this topic.

I would also like to thank Dr.Johnson Thomas and Dr.David Cline for their valuable feedback which helped me to lead my thesis in the right direction.

I would also like to thank Elaine Johns, Conferencing Manager in ITLE OSU under whom I have worked for one and half year. Her encouragement and guidance was very helpful in many ways.

I would like to dedicate my thesis to parents, Srinivasa Rao Dantala and Rajani Dantala and my brother Sravan Kumar Dantala and family members for their constant support and encouragement for me towards pursuing higher education.

I would also like to thank my friends Singi Reddy Rohith Reddy, Aileni Anvesh Reddy, Venkat Ravinder, Yashwanth Kothapalli, Sadhana Velpula, Praful Kumar, Shilpa Nanduri, Radhakrishna Kotti, Vijay Singh, Hima Bindu, Shashank Sadalia, Parmeshwar Reddy, Chakradhar Reddy, Nitesh Reddy, Siddharth Echampati, Hari Kishan Kotha Sagar Kodukula, Rohith Vaidya, Ansih Koppula and Sujith Reddy Beemireddi for their encouragement and assistance in my research.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER I

INTRODUCTION

Classical cryptography uses either public-private key pair or single secret shared key for encryption and decryption of a message. In a communication between two nodes, there is always a chance of MIM attack [1]. In the new encryption scheme for multi located parties by Kak [2], it is impossible for a localized eavesdropper to get control of the entire conversation since the points of entry and exit of data can be far apart physically.

Basically, in distributed cryptography, the objective is to share the secret among several parties, similar to a case in a bank where *k* out of *n* officers use keys simultaneously to open a vault [3],[4]. Here each party is supposed to have computers at different locations and communication among them is secure. In the simplest case, we consider each party to have one main location and a subsidiary location that we call its agent. The links between agents of different parties are not secure.

In standard cryptography we use single transformations on data whereas in multi-located parties we use transformations in sequence by several parties that guarantees the authentication. Furthermore, encrypted data can be divided into several modules or portions and sent over different channels. Multiple paths between sender and receiver make it easier to implement joint encryption and error correction coding, which cannot be achieved in such simplicity in traditional cryptography [5],[6],[7],[8].

Ad Hoc network is a collection of wireless nodes that communicate with each other in the absence of fixed infrastructure. Each node operates as both host and as a router, forwarding packets for other nodes in a network. The idea of ad hoc networking is referred to as infrastructure less networking since each node in the network dynamically establish routing among them to form their own network on the fly. Ad Hoc networks can be classified as mobile ad hoc network (MANET) and wireless sensor networks (WSN). One of the major problems in both MANET and WSN is authentication. We need an efficient protocol for authentication and to block spammers who cause unwanted network traffic and overload on nodes in a network.

Botnet is a network of compromised nodes called bots under the control of remote operator called botnet operator. Botnets pose a significant threat to distributed networks, the possible attacks with botnet are denial-of-service(DOS) attack, adware-exists to advertise some commercial things without awareness of user's, spyware-software which sends confidential information to botnet operator about user activities and email spam-receiving messages from unknown people without user permission which are either advertising or malicious in nature.

Spammers are the nodes who send spam messages without user permission, flooding the network with many copies of the same message. Basically spammers purchase services from botnet operator and send spam messages to operator, who instructs infected systems via particular server to

send out spam messages. In WSN and MANET, we propose an authentication protocol to block spammers to reduce unwanted network traffic and overload in a network

Suppose there are two nodes that are globally distributed and one node wants to transmit confidential information to other node. The major problem associated with this communication is MIM attack. The attacker or eavesdropper makes independent connections with both sender and receiver, making them believes that they are talking directly to each other over a network. In the meanwhile attacker get control of the entire conversation, observes messages exchanged from source to destination, intercepts all messages, inject new ones and transmit it to destination which effect privacy, integrity of source message. The other problem is reply attack; the attacker who monitors the conversation between source and destination captures the information and perform repeated or delayed data transmission to destination.

In Ad Hoc wireless networks such as mobile MANET and WSN, one of the problems is presence of spammers who overload the nodes in the network with spam messages without the permission of nodes. It is important to address these problems, because to protect privacy, integrity of source information and also to authenticate both sender and receiver to securely transmit information. Similarly when information exchange take place in a WSN or MANET there is need for authentication to block spammers which reduces the load and unrelated messages on each node in a network.

In this thesis, we propose a new protocol implementing authentication transformations for multi-located parties and generalization of proposed protocol to block spammers in WSN and MANET. In our approach, we assume both source and destination have subsidiary agents for carrying out authentication. The transmission of messages securely and the task of the eavesdropper is complicated by the fact that there exist multiple paths for the sender to send the information to the receiver. The proposed approach uses the concept of formal grammars and it is based on Needham-

Schroeder symmetric key protocol for classical authentication [9]. Formal grammars are used for transforming source message into a secret message, which is new way of doing encryption transformations.

In rest of the thesis, we first discuss the previous work done on three stage protocols for quantum cryptography & multi-located parties, formal grammars and blocking imposter emails using CAMEL[20] mechanism. After that we describe proposed approach of a protocol implementing authentication transformations for multi-located parties and authentication protocol to block spam messages from spammers in wireless ad hoc networks.

CHAPTER II

LITERATURE SURVEY

This chapter provides background on the several elements that go together in the thesis. This includes the three stage protocol for quantum cryptography which is the model that has been applied for classical encryption, grammars for encryption and issues related to spamming.

Three stage protocol for quantum cryptography

The system consists of sender A and receiver B who are globally distributed. Sender A has agent near B's location and receiver B has agent near A's location. Figure 1 show secure three stage protocol for quantum cryptography by Kak [16].

Protocol:

1) A→ B's agent : $V_A[M]$
2) B's agent → A's agent : $V_B V_A[M]$
3) A's agent → B : $V_A^{-1} V_B V_A[M]$
4) B finally performs transformation such that $V_A V_B = V_B V_A$

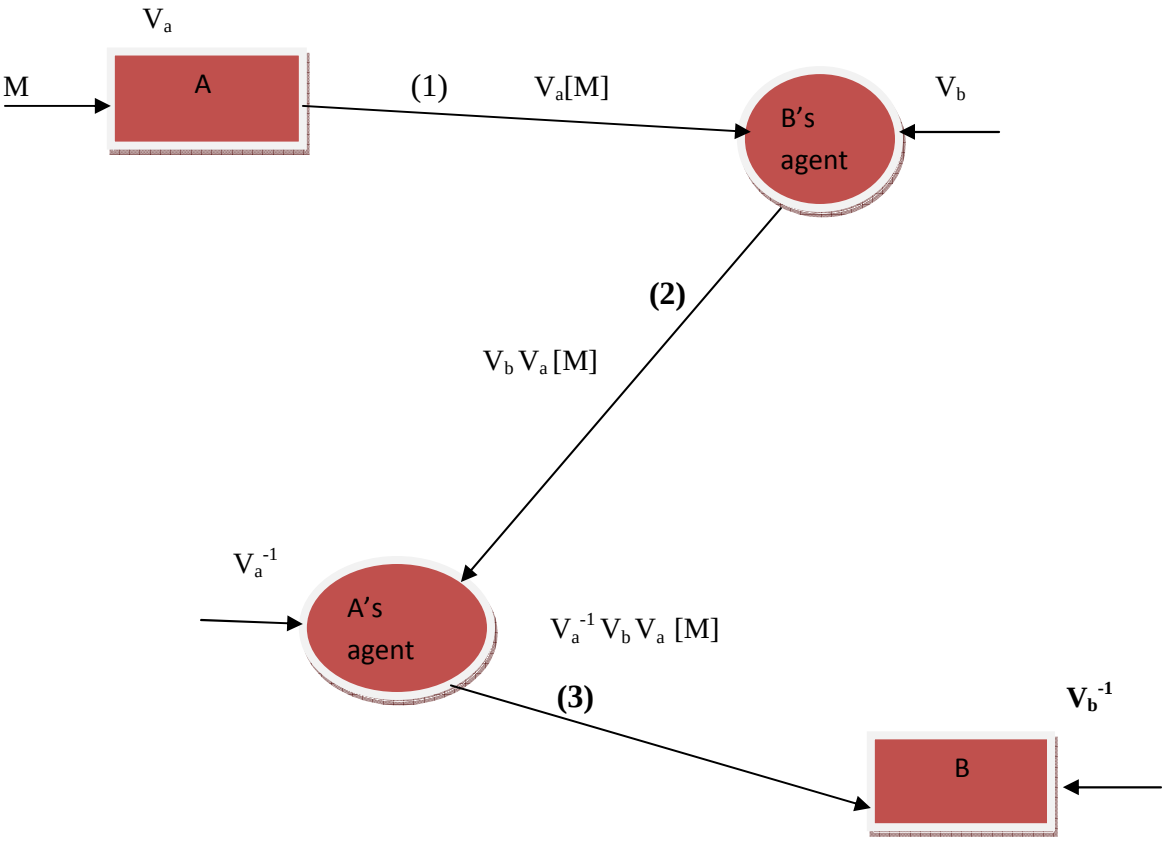


Fig-1: Three stage protocol for quantum cryptography where $V_aV_b=V_bV_a$

Observations:

A	A's agent	B	B's agent
A (V_a)	A's agent (V_a^{-1})	B (V_b^{-1})	B's agent (V_b)

In the above case, both nodes A and B do not trust each other so they use secret transformations V_a and V_b for authenticating transmissions between nodes in such a way that $V_aV_b=V_bV_a$. In this protocol, A performs transformation on message M and sends it to B's agent; B's agent also perform transformation on received message and send it to A's agent. A's agent will perform inverse transformation on received message and transfer it to B. finally B applies V_b on received

message to get the original message. In this way data is transformed securely avoiding man in the middle attack. But we observe from the protocol it resolves MIM to some extent but not full.

Here intruder pretend to be B to A and vice-versa. Instead of V_b intruder selects V_i and fakes a response which looks similar to what B would have done. Intruder pretends as A to B with the transformation V_j which is commutative to V_b and instead of M sends a message N. So from interaction with A he acquires value M and sends a junk N to Bob and hence disables the protocol. This protocol suffers from replay attack.

Three stage protocol for multi located parties

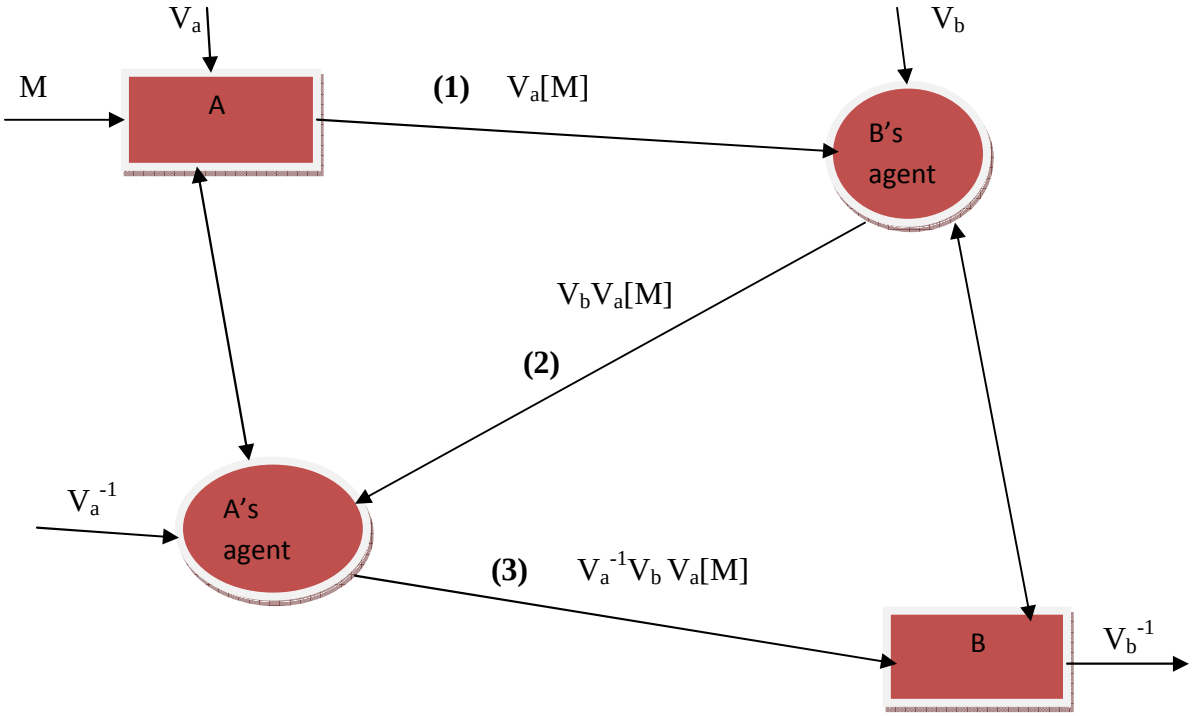


Figure 2: Three stage protocol for multi-located parties

Nodes A and B are distributed and the protocol uses multiple agents for communication between them. This protocol is same as the protocol of three stage protocol for quantum cryptography. The double arrow mark in the Figure 2 represents secure communication channel. The above protocol

works fine with the confidentiality of the message but does not provide authentication of agents and also causes replay attack.

Observations:

A	A's agent	B	B's agent
A (V_a, V_a^{-1})	A's agent (V_a^{-1})	B (V_b, V_b^{-1})	B's agent (V_b)

Linguistic Transformations using Formal Grammars

We describe grammars which may be used as a method of encryption.

A Grammar G is a quadruple (V, T, P, S) defined as follows:

V- Finite set of Non-Terminals or variables

T-Finite set of Terminals

P-Finite set of productions or rules defining a grammar

S-Distinguished non-terminal called as start symbol

Example of simple grammar:

G= ({A, B, S}, {0, 1}, {S→AB, A→0B, B→10A, A→}, {S})

Grammars may be divided into four classes by gradually increasing restrictions on the form of productions in the Chomsky hierarchy. The objective of splitting and sharing secret information is to generate the data in secret that can be shared by multiple authorized parties [11]. The general methodology using grammars for secret sharing among multiple parties [11] consists of several steps such as

1. Select a classical scheme for secret sharing

2. Convert source data in the form of bit sequences

3. Define grammar for generating secret for input message

4. Using syntax analyzer to parse the bit sequence

5. Generate sequence of grammatical rules

6. Split the secret with selected threshold scheme

7. Distribute the secret among multiple parties of the protocol

Expansion of the threshold scheme by an additional stage of converting the secret recorded in the form of a bit sequence is performed thanks to the application of context-free grammar [17].

A CFG is defined as G_{SEC}= (V_N, V_T, SP, STS), where:

V_N = {BIT, Z, O} – set of non-terminal symbols

V_T = {0, 1, λ} – set of terminal symbols which define each bit value.

{λ} – define an empty symbol.

STS = BIT - grammar start symbol.

A production set SP is defined in following way.

1. BIT → Z BIT

2. BIT → O BIT

3. BIT → λ

4. Z → 0

5. O → 1

The grammar presented here is context-free grammar [17], changing the bit sequences in the form of zeros and ones into a sequence of grammar production numbers that allow the generation of the original bit sequence. The flaws in the linguistic cryptography threshold scheme [16] are, it does not discuss about grammars other than context free grammar and no practical analysis is discussed about transformations using grammars.

In the proposed approach I practically implement transformations using grammar on source input and divide it into two pieces and can construct the original message only if you have both pieces of data and grammar to decode it.

Spamming

Spamming is the act of spreading unsolicited and unrelated content without the user permission has been observed in several domains such as email, instant messaging, web pages, wireless networks etc. Spamming is done with the use of botnet, which is a network of compromised nodes called bots under the control of remote operator called botnet operator. It can also be defined as network of software agents or robots that run automatically. The actual process of generating spam messages using botnet is described as follows:

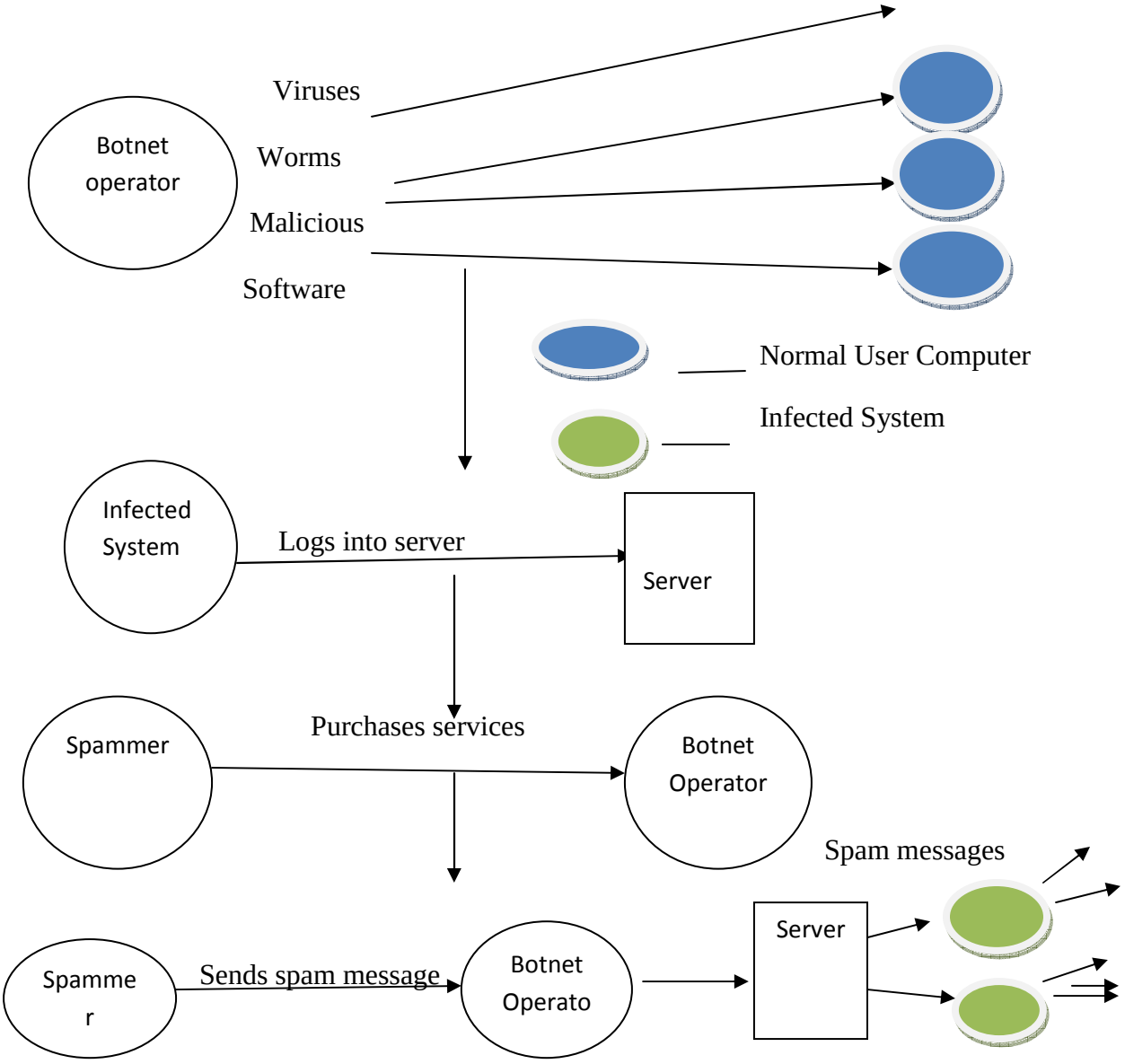


Fig 3: Botnet Process

1) Botnet operator sends viruses, worms and malicious software's to normal user computer systems.

2) The person on the infected system logs into particular server.

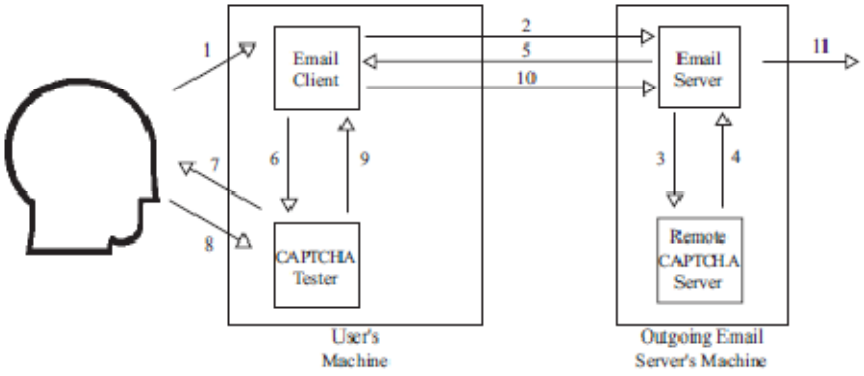
3) A spammer purchases services of the botnet from the operator.

4) Spammer sends the spam messages to botnet operator, who instructs infected systems via particular server to send out spam messages.

Blocking Outgoing Malicious Impostor Emails:

The CAMEL [20] mechanism is enforced at the legitimate outgoing email servers. It consists of profilers for the affiliated users and a RTT [18] system. A profiler can be obtained by applying an appropriate machine learning algorithm to the history data of a user. A popular RTT system is the CMU CAPTCHA [20] project.

The implementation of the CAMEL mechanism uses machine learning based profilers and the CAPTCHA system, into a standard SMTP server. The resulting system consists of two computers connected to a 100M Ethernet LAN: one machine Hermes acted as the user's machine using an email client called Pooka [19], and another machine Jupiter acted as the outgoing email server's machine using the send mail server version 8.12.9. Both machines run the Linux operating system.



\

Fig 4: Camel Mechanism

Camel mechanism has the following steps to block outgoing imposter emails.

1. The user composes an email using the email client.

2. The email client requests the email server to send the email.

3. Suppose the request does not pass the profiler. The email server asks the CAPTCHA server to generate a CAPTCHA challenge.

4. The CAPTCHA server returns a challenge and its answer.

5. The email server responds to email client with the CAPTCHA challenge.

6. The email client calls the CAPTCHA tester to deliver the challenge.

7. The CAPTCHA tester delivers the challenge.

8. The CAPTCHA tester collects the user's answer.

9. The CAPTCHA tester forwards result to email client.

10. The email client passes the result to email server.

11. The email server verifies the result of the challenge. If the result is correct, the email server sends the email to the recipient as in the original system; otherwise, the request may be dropped or re-challenged (depending on the system policy).

We practically implemented a new way of transformations based on formal grammars to generate a secret from an input message. When two parties are globally distributed, each of them is associated with a subsidiary agent. Using these subsidiary agents for authentication and secure transmission of information from source to destination is a new concept that has been proposed.

Standard methods perform transformations on input messages and send them on to destination. In my approach, after performing transformation using grammars or any other techniques on input message the source will break the secret into two parts and transmit it to two subsidiary agents. This will help avoid man in the middle attack because the task of the

eavesdropper is complicated by the fact that there exist multiple paths for the sender to send the information to the receiver. We also propose a new protocol to block spam messages in WSN and MANET based on authentication transformations, breaking secret into two parts.

Detection method of dynamic spammer's behavior

The spam detection algorithm uses three types of graphs which are directed, undirected and a differential graph which is obtained from results of two directed graphs.

Directed graph of email exchange activity is given as

$D = (N, A)$

Where N represents set of all email users and A represents set of arcs corresponding to each pair of email users.

Undirected graph is defined as $G = (V, E)$

Where V is set of all email users and E is set of edges corresponding to a pair of users.

Differential graph is built from two directed graphs $D_1 = (N_1, A_1)$ and $D_2 = (N_2, A_2)$ such that

$D^d = (N^d, A^d)$

The three stages spam detection algorithm [21] consists of following 3 procedures

1) Procedure A: Builds graphs from system server's log files, these graphs are called as email graphs. Through these graphs it is easy to find relationships between email users to whom the potentially unsolicited email is directed.

2) Procedure B: Initially classifies each sender of e-mails as spammer (black list (BL)), regular user (white list (WL)) or unknown user (grey list (GL)) examining the properties of the two previously defined graphs (directed and undirected) built for one consecutive

period of time. Additionally a group of previously defined sub graphs are taken into account. The sub graphs represent typical spammers and non-spammers behavior.

3) Procedure C: Refines the initial classification done by the procedure B.

The refinement procedure promotes or demotes each sender based on following properties

1) Email traffic generated towards sender.

2) Email traffic registered in the previous period of time.

3) The first promotion can occur if the sender looks suspicious (after the initial classification being located on BL or GL) and the recipient responded to the e-mail sent by the sender. The response will lend credence to this relation and will move the sender from BL to GL or from GL to WL.

The sender can also be promoted or demoted based on result of the comparative analysis included in procedure C. Comparative analysis considers the history of e-mail exchange between the sender and recipient. It uses a differential graph that has to be build for two disjunctive periods of time. The presence of the arc in the differential graph between the nodes representing the sender and the recipient indicates that either the recipient started a new relation with the sender or the sender is a spammer. According to this assessment the sender is promoted (if it did send an e-mail in the past to the recipient) or demoted (in other case).

The spam detection algorithm is used in procedures B and C to separate spam messages from regular e-mails. The algorithm is parameterized that makes it easy to adapt to constantly changing spammers behavior. It classifies each incoming e-mail on-line in four steps:

- It inserts the appropriate link to the graph representing each exchanged e-mail

- Initially classifies the e-mail sender as a member of BL (blacklist), GL (gray list) or WL (white list). This classification is based only on the information collected for the second period of time. Mainly it uses sub graph patterns and the properties of the directed and undirected graphs built for this period.

- Refines the sender classification taking into account e-mail traffic towards the sender and historical data represented by a differential graph. In fact every link from the sender to a local user assesses the sender to be classified on BL, GL or WL. The sender is finally classified on a specified list taking into account all the assessments.

- Classifies the e-mail according to the classification of the sender

CHAPTER III

METHODOLOGIES

When two parties are globally distributed, one party wants to transmit confidential information to other. There is always a probability that an eavesdropper will get control of the entire conversation, the eavesdropper does so by making independent connections with both sender and destination by pretending to the sender that he is destination and to the destination that he is sender resulting in attacker gaining confidential information, injecting new message and transmit it to destination. This attack is defined as MIM attack.

The other possible attack is replay attack. Here the attacker monitors the conversation between source and destination, records the information and performs repeated or delayed data transmission to destination.

Spamming is sending unrelated content without user permission. Spamming make use of botnet, botnet is network consisting of compromised nodes under the control of botnet operator. In WSN and MANET, spammer generates spam messages and overloads nodes, increase network traffic, delivering unrelated messages.

This section discusses the proposal of new three stage protocol implementing authentication based on Needham-Schroeder protocol and transformations based on linguistic

transformation using grammars to avoid MIM attack and replay attack providing privacy, integrity of a message for multi-located parties. Later we propose an authentication transformation protocol for WSN and MANET to block spam messages from spammers in a network.

Proposed protocol implementing Authentication Transformations for Multi-Located Parties:

Description of protocol

1. Node A → BB: V_{AB}

   Node A→AA: V_{AA}

   Node A → KDC: E (K_A, [ID_A, ID_B, N_a])

2. BB → KDC: E (K_B, [ID_B, N_b, T_b,V_{AB}])

3. KDC → AA: E (K_A, [ID_B, N_a, T_b, K_s])|| E (K_B, [ID_A, Ks, V_{AB}])

4. AA → Node B: E (K_B,[ID_A, Ks, V_{AB}])||E (Ks, [Nb, V_{AA}])

5. Node B: ($V_{AA}V_{AB,}$ G) → Input message

Figure 3 depicts the following steps for multi-located parties:

1) Node A performs transformations using grammar and divide it into two parts $V_{AA,}$ V_{AB} and send V_{AA} to AA and other to BB and encrypted information of ID's of nodes A & B with a nonce Na to KDC using shared key K_A between node A and KDC.

2) BB sends encrypted form of information containing his ID, nonce Nb and time stamp Tb along with V_{AB} to KDC using shared key K_B between BB and KDC.

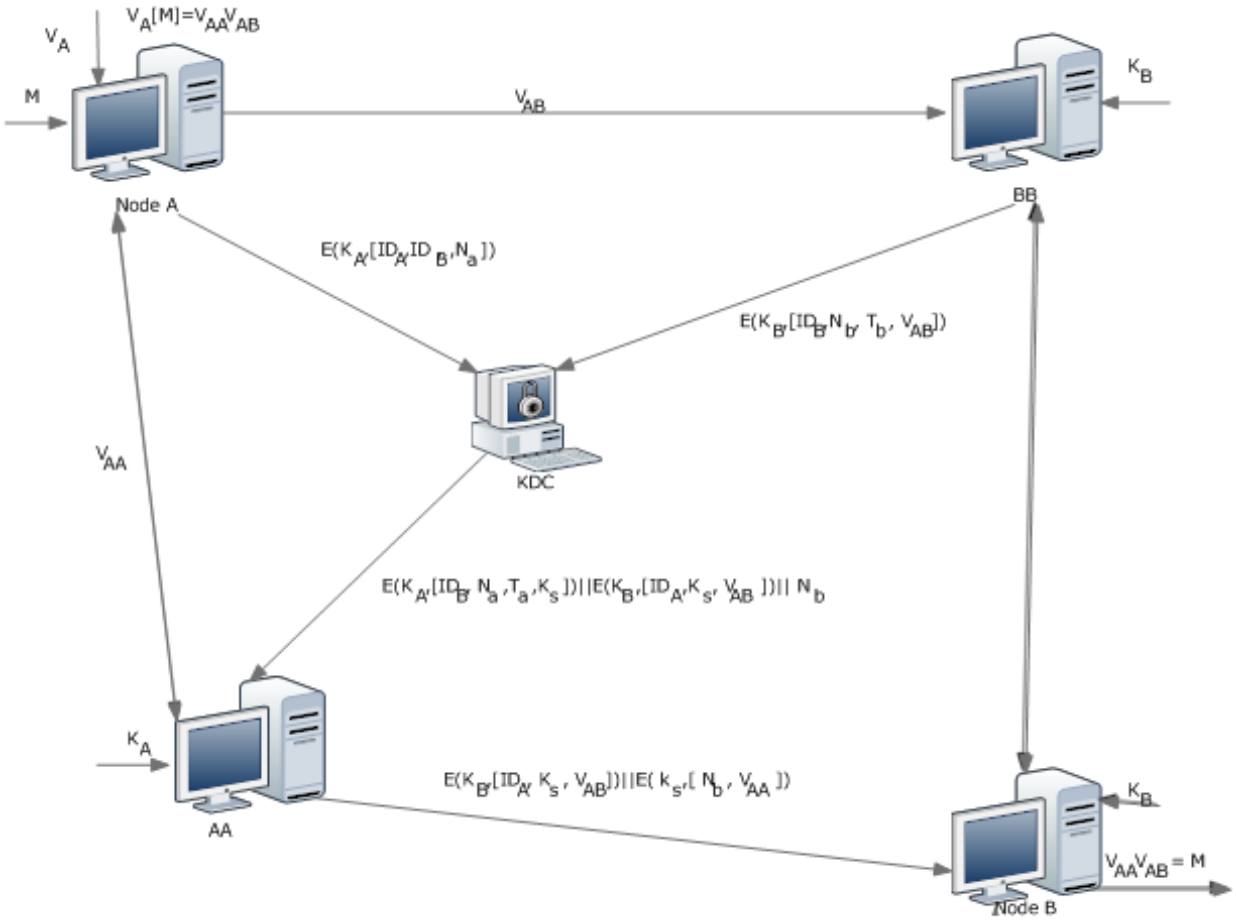


Figure 5: Protocol implementing authentication and linguistic transformations for multi-located parties

3) KDC assigns a session key and send information to AA containing identity of B, nonce Na, time stamp Tb and session key Ks which is encrypted using A's key K_A and information containing identity of A, a session key and V_{AB} which is encrypted using B's key K_B.

4) AA receives his nonce Na back and A is assured of timeliness by the session key and ensured that it's not a replay. AA send information containing ID of A, session key Ks and V_{AB} which is encrypted using B's key K_B and encrypted form of nonce Nb and V_{AA} using session key Ks.

5) Finally, B receives two parts V_{AA} and V_{AB} and combines both. B use $V_{AA}V_{BB}$ and grammar to reveal the secret.

Observations:

A	AA	B	BB
A (V_A[M], $K_{A,}$ grammar, bit sequence number)	AA (K_A)	B ($K_{B,}$ grammar, bit sequence number)	BB (K_B)

In Figure 4, sender A performs linguistic transformations on input message to produce V_A [M]. Sender A will break transformed message into two parts V_{AA}, V_{AB} and transmit it to two agents AA and BB. BB encrypts message V_{AB} and send it to AA, who in turn send both V_{AA}, V_{AB} to destination B.

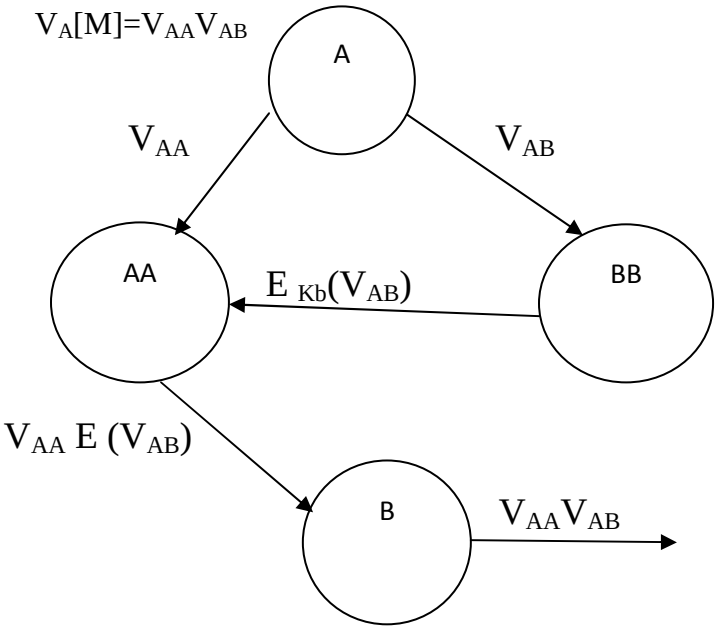


Figure 6: New protocol for linguistic transformations and secret sharing for multi-located parties

Sender A performs linguistic transformations using grammars to convert a message into production sequence numbers. Destination B uses production sequence numbers and grammar to reveal the secret.

Example: Linguistic transformations using grammars on input message

Input Message: “hello”
↓
Converting message into bits using 7 bit sequence:1000011101001100110111111011
↓
Sender A- select bit sequence(e.g. 3 bit sequence): 100001110100110011011111011
↓
Sender A-select any type of grammar(e.g. context free grammar using 3 bit sequence)
G=({S,A},{0,1},P, {S})
Where P is defined as follows
1 S→BB
2 B→AB
3 B→€
4 A→000
5 A→001
6 A→010
7 A→011
8 A→100
9 A→101
10 A→110
11 A→111
↓
Use grammar to convert bits into production sequence number:1282521028272112=V_A[M]

Analysis of protocol

For two parties, A and B, that are globally distributed and want to exchange information among them, there are two other parties namely AA for A’s agent and BB for B’s agent, who participate to securely communicate information from source to destination. As discussed in the previous section, presence of KDC allows all the parties to authenticate and validate themselves before

transmission. Since sender A performs transformations on input message using grammars, we will get a message that represents production sequence numbers. The most important part of the proposed protocol is that A breaks the transformed message into two parts and transmits these two parts to AA and BB.

Since AA or BB know neither the grammar nor complete transformed message, they cannot construct the original message and also it is difficult for intruders to obtain the secret since transformed message is divided into parts and transmitted separately, avoiding MIM attack.

Finally, rather than basing security on direct communication between two parties, the proposed protocol uses the concept of multiple parties between source and destination making it possible to obtain higher level of security. When two parties are globally distributed, this protocol can be implemented in a simple and secure manner.

Authentication protocol to block spam messages in wireless ad hoc networks

Generalization of above proposed approach to block spam messages from spammers in wireless ad hoc networks.

In both WSN and MANET, spamming causes network overload and storage of unrelated information on sensor nodes or mobile nodes. To avoid these difficulties we need to modify WSN and MANET with addition of some authentication agents.

Modified Networks with authentication protocol

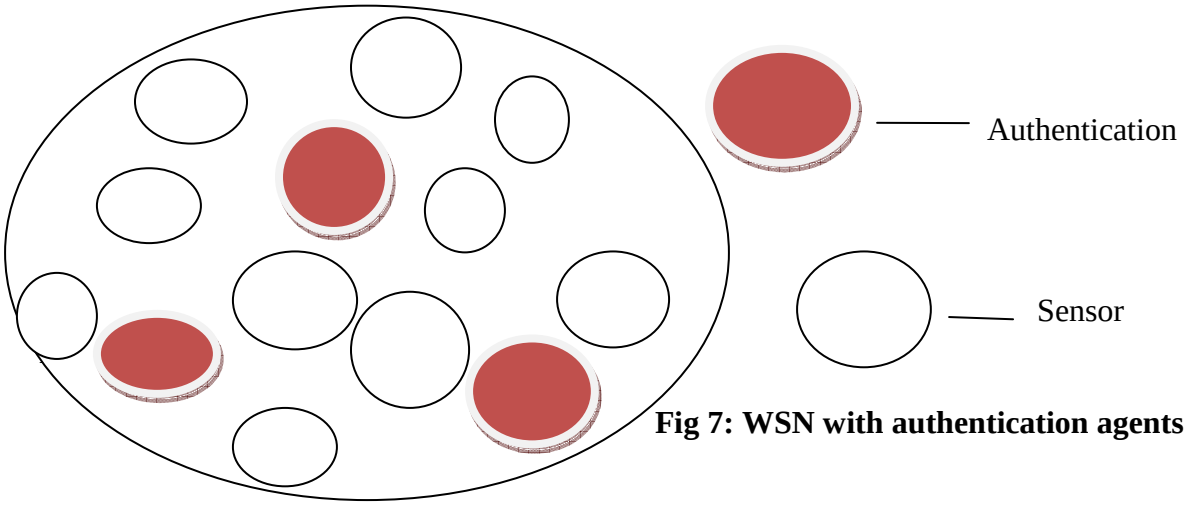


Fig 7: WSN with authentication agents

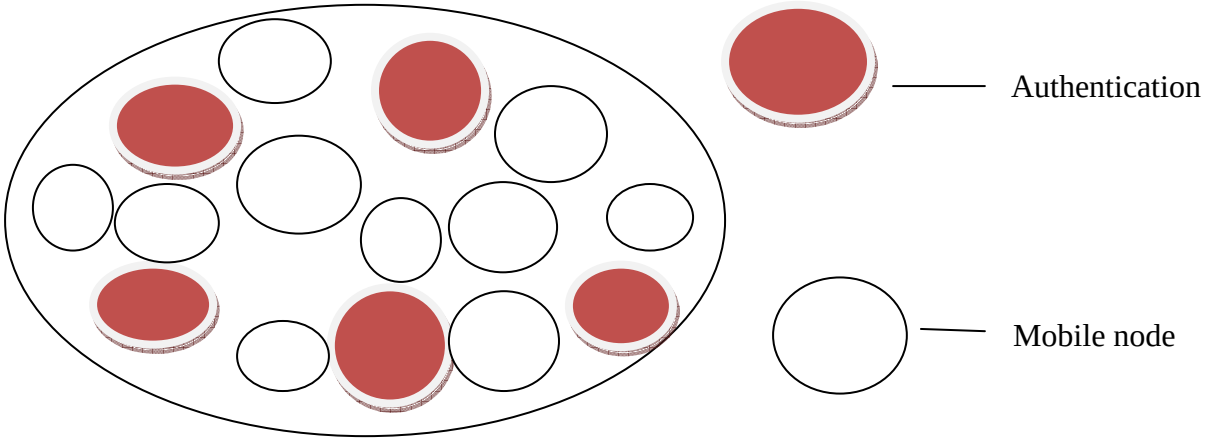


Fig 8: MANET with authentication agents

The proposed approach assumes ad hoc networks such as WSN and MANET with more than one authentication agents. The number of authentication agents to choose depends up on number of nodes in a network. I simulate the probability of choosing authentication agents for a network at later stage. In this scenario to block spam messages from spammers, we propose an authentication protocol which is described as follows:

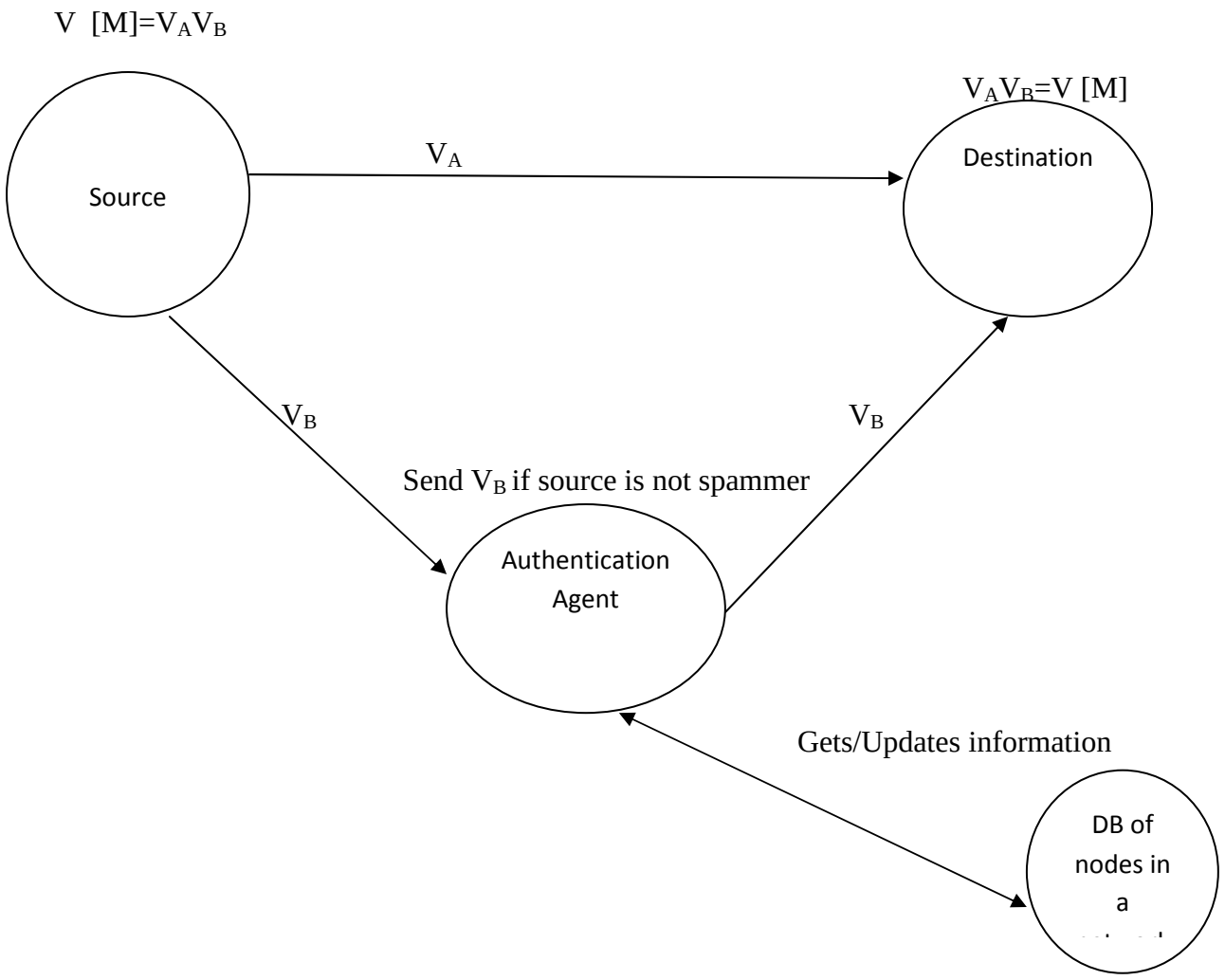


Fig 9: Protocol to authenticate nodes and block spam messages from spammers

The above figure depicts the proposed protocol to block spammers in wireless ad hoc networks. Consider a spammer wants to send spam messages in a network, unlike sending messages directly from source to destination the proposed protocol uses authenticating agents in the network.

The wireless ad hoc network consists of nodes and some authenticating agents based on the size of the network. Each network is assumed to have 1 database (DB) node which maintains database of node information such as node ID, number of redundancy messages, node behavior, spam messages etc. Only authentication agents have access to DB node, they can update information and request information from DB node. Any node to communicate or send messages to other nodes in a network, first it has to communicate with authentication agent.

The task of authentication agent is to check validity of node, previous node behavior and messages, number of redundant messages sent in the past etc through access from DB node. Before transmission of message, a process similar to handshake Protocol takes place between sender and receiver to avoid replay attack, denial-of-service attack (DOS) and to reduce overload on authentication agents and overflow of messages in a buffer.

The process consists of the following steps, sender sends information such as node ID and nonce to authentication agent; the authentication agent gets information about node from node DB and it checks node behavior. The nonce is used to avoid replay attack and denial-of-service attack.

Since the message is not transmitted before handshake protocol, it ensures that buffer used for transmission is not overloaded and reduces delay with authentication agents.

Protocol:

1. Source: V [M] = (70% of V [M]=V_A).(remaining 30% of V [M]=V_B)
2. Source → Destination : V_A

   Source → Authentication agent: V_B
3. Authentication agent :

```
If (source is spammer)
  {
      Block V_B to destination;
  }
else
```

{

Allow V_B to destination;

}

4. Authentication agent→ Destination: if(valid node) then V_B else informs source is spammer.

5. Destination: $V_A V_B$=V [M]

Description of the protocol

1) The message M which source wants to transmit is transformed to integers V [M] using formal grammars.

2) V [M] is divided into two parts V_A and V_B.

3) Here we divide V [M] in such a way that 70% of V [M] is V_A and remaining 30% is V_B to reduce load on authenticating agents.

4) Authentication agents maintain information and behavior of nodes such as repetition of same message to many nodes etc.

5) One part of the message V_A is transmitted to destination and other to authenticating agent, where authentication agent verifies the ID of source and get the related information about that node, if the node is spammer then it blocks the message V_B otherwise send V_B to destination.

6) Whenever both $V_A V_B$ are combined then only message is delivered to destination otherwise it's a spam message and message is blocked by authentication agent.

Analysis of protocol:

In both WSN and MANET nodes which are compromised can act as spammers. Spammers generate spam messages and send same copy of message to many nodes in the network. The proposed protocol solves the problem by adding authentication agents to the network based on the size of the network. These authentication agents keep track of ID's of nodes, node information such as previous messages sent by node and validity of the node etc through access from node DB. Before applying transformations and transmission of message, a process similar to handshake protocol takes place between sender and authentication agent to avoid replay attack, DOS, overloading of messages and delay with authentication agent.

This approach does not allow messages to be transferred directly to destination. Instead, it breaks the message into two parts. One containing 70% of message is transmitted to destination node and remaining 30% of message is transmitted to authentication agent. In order to reduce load on authentication agents we send the smaller part to it. The agents check the identity, validity and complete source node information. If it finds source node to be valid then only it sends remaining 30% of message to destination. When both parts are combined it is delivered to destination, otherwise it is not delivered.

If the authentication agent finds source node to be a spammer then it blocks the message. As it is not delivered to destination, both parts are not combined prevents in spam messages from reaching the destination. This reduces the node overhead, network traffic, avoiding unrelated message delivery without permission.

Comparative Analysis

Comparing proposed authentication protocol for multi-located parties with already established protocols, the proposed protocol is more secure than previous ones and it avoids man-in-the-middle attack.

We modified Kak's cryptography for multi-located parties with the addition of a secret sharing scheme which divides a message into two parts are transmitted to two agents, the use of a key distribution center to securely establish a session key between source and destination, nonces and time stamps. Through this modification higher level of security is guaranteed. The use of time stamps and nonces avoid replay attack which makes the protocol even stronger to break.

The proposed authentication protocol for wireless networks to avoid spamming is more efficient than previous protocols. Blocking outgoing malicious imposter emails by Erhan uses CAMEL mechanism which is enforced at the legitimate outgoing email servers. Machine learning algorithms are applied to the history data of user to get the profiler. Whenever email client request does not pass the profiler at server then email server asks the CAPTCHA server to generate a CAPTCHA challenge. This challenge has to be cleared by email client to email server.

The drawbacks of the Erhan's protocol are delay in the process of verification and network overload and buffer overflow. Our proposed protocol side steps many of these difficulties. By using secret sharing scheme of dividing message into two parts it is difficult for intruders to gain the message. Authentication agents are used for verification in wireless network to block spammers. Dividing message into two parts avoids buffer overflow. It uses a near uniform distribution of authentication agents to reduce network traffic.

CHAPTER IV

FINDINGS

Probability of selecting authentication nodes for a network of 200 nodes

I considered a network of 200 nodes with 5, 10 and 15 authentication nodes. The network was represented by its adjacency matrix. A random number generator (RNG) was used to determine the number of accesses to each authentication node. I observed that for 5 and 10 authentication nodes, number of accesses to authentication nodes varies more compared to network with 15 authentication agents. I simulated for 200 nodes and find if there are greater than 15 authentication nodes the number of accesses varies a lot as shown in the graphs. Our objective is to ensure that the load on all the authentication nodes is as uniform as possible.

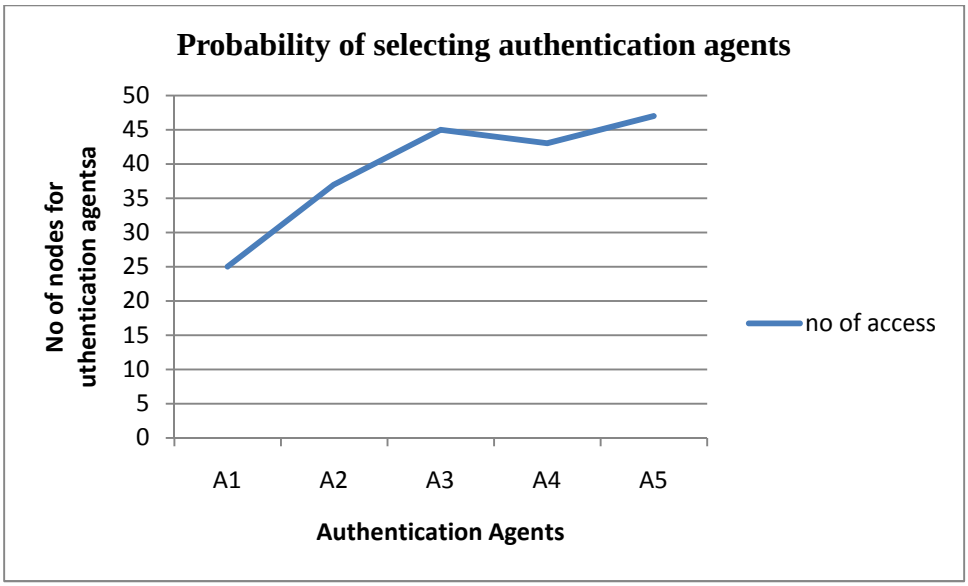


Fig 10: 200 nodes with 5 authentication agents

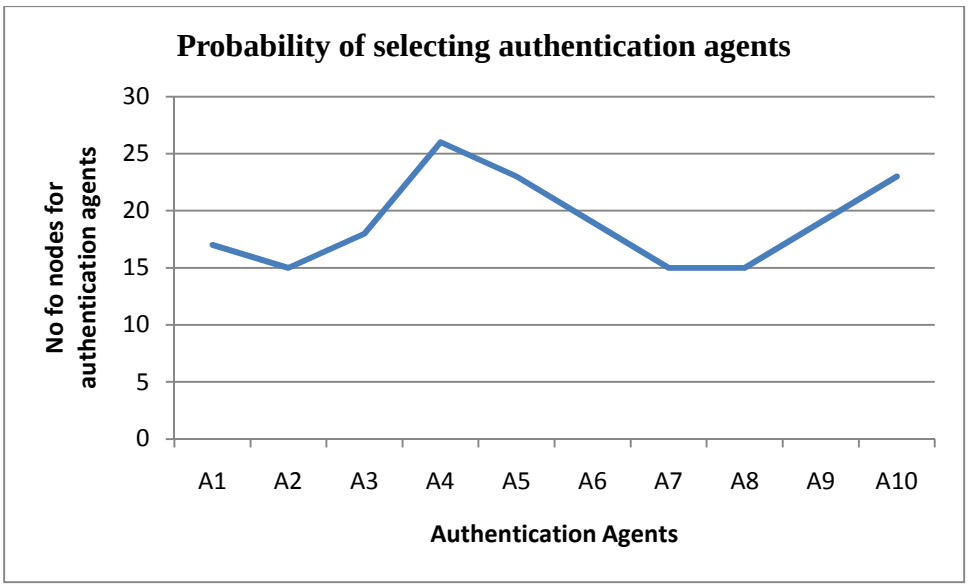


Fig 11: 200 nodes with 10 authentication agents

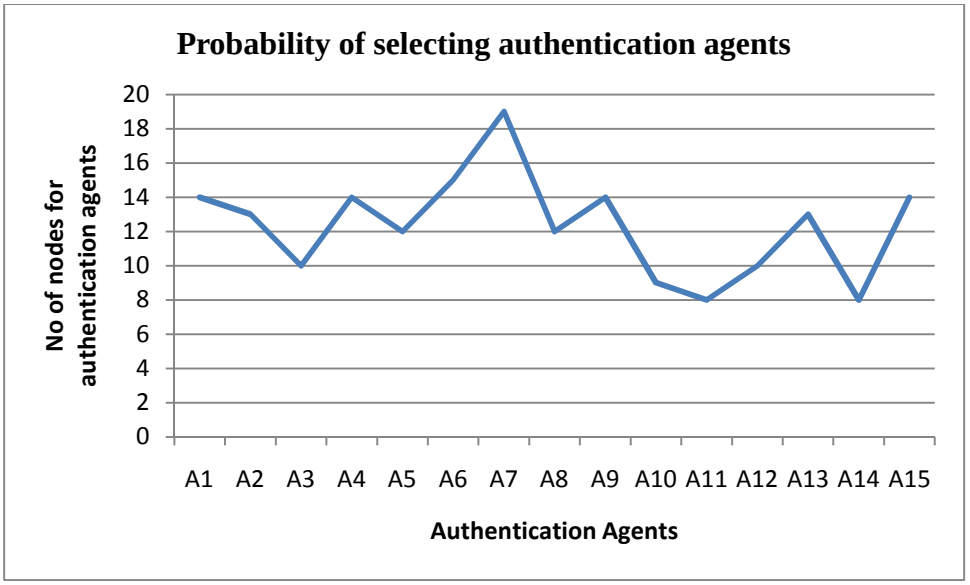


Fig 12: 200 nodes with 15 authentication agents

As shown in figures 13 – 16, the choice of 0.075 probability for the number of authentication nodes provides reasonable degree of uniformity of workload on the authentication agents.

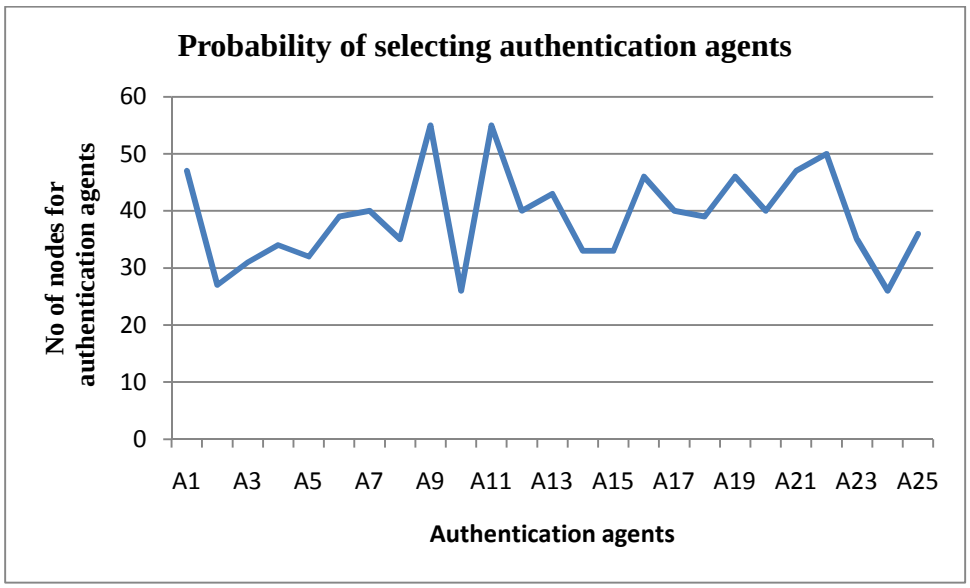


Fig 13: 1000 nodes with 25 authentication agents

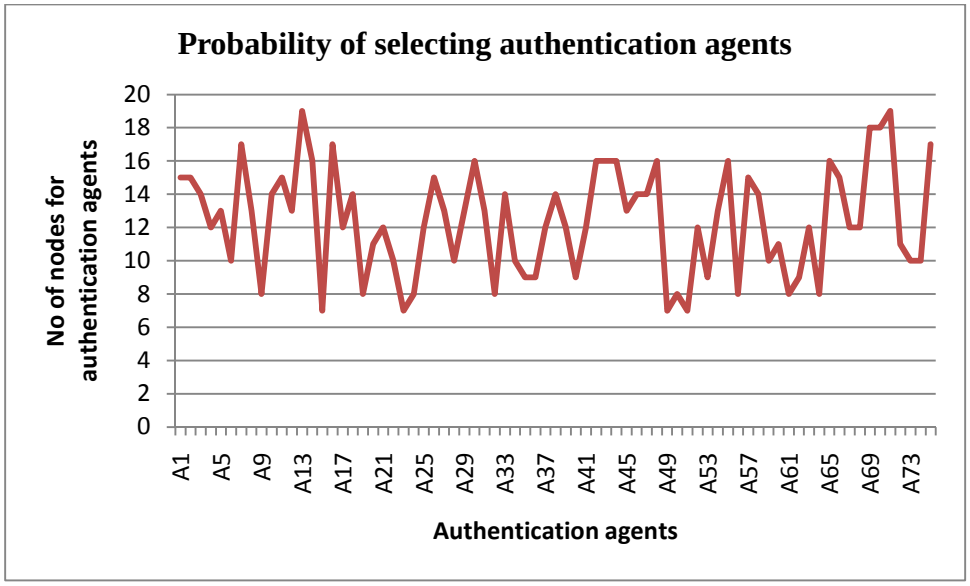


Fig 14: 1000 nodes with 75 authentication agents

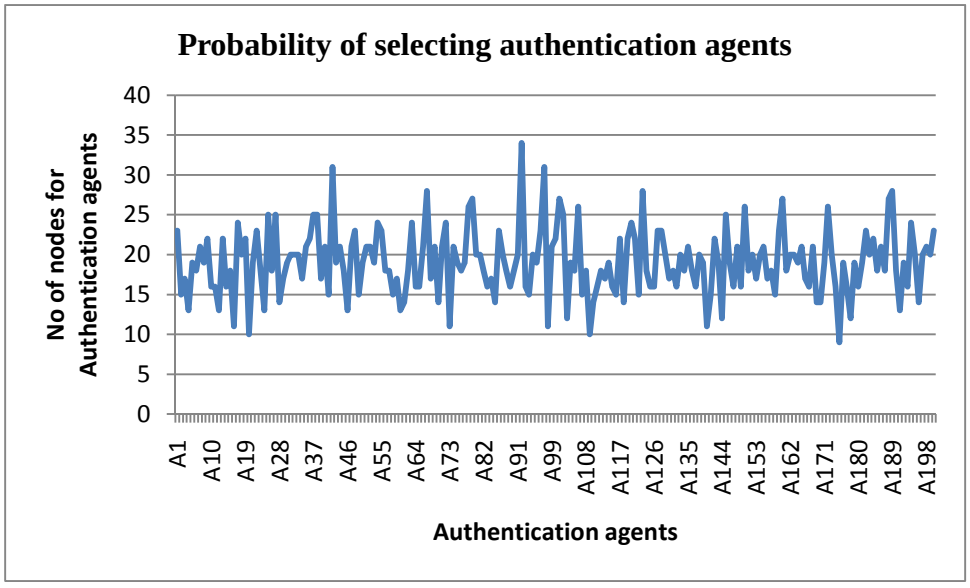


Fig 15: 4000 nodes with 200 authentication agents

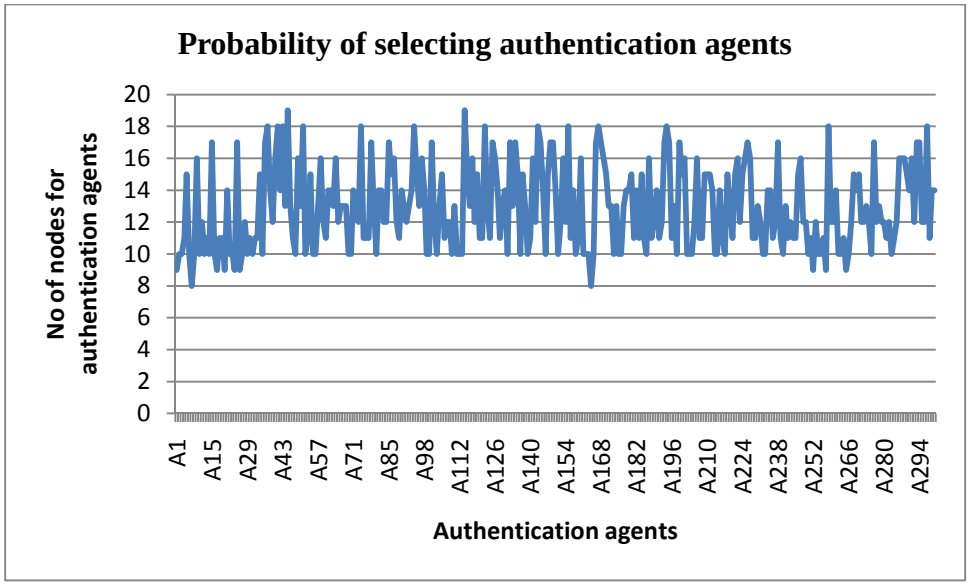


Fig 16: 4000 nodes with 300 authentication agents

CHAPTER V

CONCLUSION

In this thesis, we used the three stage protocol for multi-located parties as starting point to develop an agent based authentication system. We assume both sender and destination have agents for carrying out authentication and transmission of messages securely. We implemented transformations on input messages using formal grammars and other techniques which generate encrypted message of integers.

We implemented a protocol that divides input transformed message into two parts and passes them to two subsidiary agents of source and destination so that the message reaches destination securely. The task of the eavesdropper is complicated by the fact that there exist multiple paths for the sender to send the information to the receiver.

The concept of dividing the message may be used on a wireless ad hoc network to avoid flow of spam messages and to block spammers in the network. When sender transmits a message to destination, the protocol transforms the message and divides it into two parts in such a way that only a small part of message is stored in buffer at destination and major part is stored at authentication nodes. The authentication nodes block spammers which reduce network traffic and

overload in a network. We simulated a static network of 200, 1000, 2000 and 4000 nodes to find out the number of authentication nodes to be chosen so that access to authentication is uniformly distributed. Through simulations we found that 0.075 probability is a good number for authentication nodes to be used in the network.

This authentication protocol works well in a static network. We do not know how well it will work if implemented on a dynamic network.

REFERENCES

1. B. Schneier, Applied Cryptography, John Wiley, New York, 1996.
2. S. Kak, "Cryptography for multi located parties." Cryptography and Security, 2009. arXiv:0905.2977v1.
3. P. Rogaway and M. Bellare, Robust computational secret sharing and a unified account of classical secret-sharing goals. ACM Conference on Computer and Communications Security, pp 172–184, 2007.
4. V. Vinod, A. Narayanan, K. Srinathan, C. P. Rangan, and K. Kim, On the power of computational secret sharing. Indocrypt *2003*, vol. 2904, pp. 265–293, 2003.
5. S. Kak and A. Chatterjee, On decimal sequences. IEEE Transactions on Information Theory, IT-27: 647 – 652, 1981.
6. S. Kak, Encryption and error-correction coding using D sequences. IEEE Transactions on Computers, vol. C-34, pp. 803-809, 1985.
7. S. Kak, New results on d-sequences. Electronics Letters, 23: 617, 1987.
8. A. Parakh and S. Kak, Online data storage using implicit security. Information Sciences, vol. 179, pp. 3323-3331, 2009.

9. R. Needham and M. Schroeder, Authentication Revisited. Operating Systems Review." January 1987.
10. S. Kak, On secret hardware, public-key cryptography. Computers and Digital Technique (Proc. IEE - Part E), vol. 133, pp. 94-96, 1986 .
11. Marek R. Ogiela, Urszula Ogiela, Linguistic cryptography threshold schemes. International Journal of Future Generation Communication and Networking Vol. 2, No. 1, March, 2009
12. K. Park and H. Lee. "On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack." Tech. Rep. CSD-00-013. Purdue University. June 2000.
13. S. Kak, On the method of puzzles for key distribution. Intl. Journal of Computer and Information Science, vol. 14, pp. 103-109, 1984.
14. M. Gnanaguruparan and S. Kak, Recursive hiding of secrets in visual cryptography, *Cryptologia*, vol. 26, pp. 68–76, 2002.
15. A. Parakh and S. Kak, A recursive threshold visual cryptography scheme, *Cryptology ePrint Archive, Report 535*, 2008.
16. S. Kak, 2006. A three-stage quantum cryptography protocol. Found. Phys. Lett. 19: 293- 296; arXiv: quant-ph/0503027.
17. M.R. Ogiela, R. Tadeusiewicz, Modern Computational Intelligence Methods for the Interpretation of Medical Images, Springer-Verlag, Berlin Heidelberg, 2008
18. M. Naor. Verification of a human in the loop or identification via the turing test.

http://www.wisdom.weizmann.ac.il/~naor/onpub.html

19. A. Petersen Pooka: A Java Email Client.http://suberic.net/pooka

20. Erhan J. Kartaltepe, Shouhuai Xu. ”Towards Blocking Outgoing Malicious Impostor emails”, WoWMoM 2006. International Symposium on aDigital Object identifier: 10.1109/WOWMOM.2006.109 , pp-661, IEEE, 2006.

21. R.Brendel, H.Krawczyk, “Spam classification methods based on users’ e-mail communication graphs”, Proc. Of The Second IEEE International Conference on Technologies for Homeland Security and Safety, Kadir Has University 2006.

VITA

PRADEEP KUMAR DANTALA

Candidate for the Degree of

Master of Science

Thesis: AUTHENTICATION FOR MULTI-LOCATED PARTIES AND WIRELESS AD HOC NETWORKS

Major Field: Computer Science

Biographical:

Education:

Completed the requirements for the Master of Science in Computer Science at Oklahoma State University, Stillwater, Oklahoma, US in July 2011.

Completed the requirements for the Bachelor of Technology in Computer Science & Engineering at Jawaharlal Nehru Technological University, Hyderabad, Andhra Pradesh, India in May 2009.

Experience:

Graduate Assistant — January 2010 – May 2011
ITLE, Oklahoma State University — Stillwater, Oklahoma

- Used camtasia for recording, editing, posting media files online which include lectures, seminars and conferences.
- Converted different media formats for online viewing using tools such as avs video converter and windows media editor.

Information Technology Intern — June 2011 – Present
Sonic Corporate — Oklahoma City, Oklahoma

- Setting up virtual WYSE terminals using VMware, AS400 operations for a corporate staff of 400 members.
- Assisted technical support and troubleshoot in software issues such as outlook, excel and hardware issues such as VMware, printers, fax and networking issues such as unlocking user accounts, AS400 operations, VPN and virus related issues.

Teaching Assistant — August 2010 – May 2011
Computer Science, Oklahoma State University — Stillwater, Oklahoma

- Designed assignments in IJVM, java, Php and Mysql databases.

Name: Pradeep Kumar Dantala Date of Degree: July, 2011

Institution: Oklahoma State University Location: Stillwater, Oklahoma

Title of Study: AUTHENTICATION FOR MULTI-LOCATED PARTIES AND WIRELESS AD HOC NETWORKS

Pages in Study: 38 Candidate for the Degree of Master of Science

Major Field: Computer Science

Scope and Method of Study:

This thesis present a new authentication protocol for multi-located parties which uses an agent based scheme that divides the message into two parts together with a key distribution center to ensure stronger authentication. It also presents a protocol for wireless ad hoc networks to combat spamming and reduce traffic overload.

Findings and Conclusions:

The appropriate number of authentication agents was calculated for a wireless ad hoc network. Simulations were run for networks of 200, 1000, 2000 and 4000 nodes and it was found that 0.075 n (n is the number of nodes in the network) authentication agents work well to distribute the load evenly amongst them.

ADVISER'S APPROVAL: Dr. Subhash Kak