International Journal of Current Trends in Engineering & Research (IJCTER)
e-ISSN 2455–1392 Volume 2 Issue 2, February 2016 pp. 32 - 40
Scientific Journal Impact Factor : 3.468
http://www.ijcter.com

Secure Group Communication using Keller box method based on first order derivatives in a Peer - to - Peer Network

Koduganti Venkata Rao[1], S.V.P.K.Satya Dev[2]

[1]Professor in CSE, [2]Asst. Prof. in CSE
[1,2]Department of Computer Science and Engineering,
Vignan's Institute of Information Technology, Duvvada, Visakhapatnam, India

Abstract—Securing Group Communications has become a critical Networking Research Issue. As data communications over massive internetworks increases, the information becomes more susceptible and sensitive. Many developing applications focus on security and confidentiality, so this demand upshot the efficiency of the bandwidth. Hence efficiency is provided by the proposed method called Keller-Box method. It is a mathematical scheme used to solve complex numerical problems to get precise and feasible solution which can be also advantageous for security issues.

Keyword—secure group communication, Keller box method, point to point communication, multipoint communication, multicast security, Peer - to - Peer networks, Newton's method.

I. INTRODUCTION

Now a days, Internet usage has been rapidly increasing day by day. In this fast-forwarding era, internet is used for Data Communication, Data Transfer, Data Storage, Data Research, Data Accessing, Data Retrieval, Data Modification, Data Sharing, Data Privacy etc. Due to this massive distribution of data, traffic and demand increases which leads to innovative thoughts and ideas. These ideas result in new applications like Teleconferencing, Information Services, Pay-Per-View, Video-On Demand etc. and technologies like Virtual desktops, SaaS Management and Testing etc. These emerging technologies will effect group communications making critical by rising different issues like Authentication, Confidentiality, Integrity, and Reliability etc. To reduce such issues, many techniques like Encryption, Decryption, Cryptography, Steganography, Group Key Management, etc are developed and enriched with new rising technologies.

1.1 Group communication:

A communication that occurs in an assemblage of persons or objects, all interconnected and capable of communicating with each other is called Group Communication. The Group communication is of two types:

1) **One-to-Many Relationships:** This represents one-Sender to many-Recipients. In this case, one entity acts as a sender and all others are recipients.
   Ex: Data distribution, Streamed data delivery, Software distribution.
2) **Many-to-Many Relationships:** This represents many-Senders to many-Recipients. In this case, each entity acts as both sender and recipient.
   Ex: Distance learning, e-learning, Audio/Video conferencing.

1.2 Secure group communication:

The Group communication which is securely isolated from all other users on the network is called Secure Group Communication. The secure group communication provides two types of configurations:

1) **Point-To-Point:** The communication between one system to another system. All the data transmitted and accessed is only within these two systems in absence of the third party. This connection is limited to two nodes in a network. It is also known as *Unicast*.
   Ex: PSTN (Public Switched Telephone Network), Hub and spoke.
2) **Multipoint:** The communication between two or more systems. All the data transmitted and accessed is within only these systems in a network. It is known as *Multicast*.
   Ex: MBONE (multicast bone), Full Mesh/Partial Mesh.
   If the communicating channel fails in point to point, then data loss highly happens. But in multipoint, the rate of data loss is less as it is replicated in other systems as well.

1.3 Multicast security:

The Multicast Network communications has become important for distributed and group based applications. So with this increasing communication support, security is in stake. The Primary objective of a multicast security infrastructure is to maintain secrecy and guarantee authentication for all group communications so that only legitimate senders can multicast packets to the group and only packets sent by legitimate group members are accepted. Consequently like unicast, Multicast group communications are also in provision to security services like Confidentiality, Integrity, Authenticity, Availability as well as Non-Repudiation.

- **i) Confidentiality:** It ensures that classified information in the network is never unveiled to unauthorized entities.
- **ii) Integrity:** It guarantees that a message being transferred between nodes is never altered or corrupted.
- **iii) Availability:** It infers that the requested services (e.g. bandwidth and connectivity) are available in well-timed even though there is a potential problem in the system.
- **iv) Authenticity:** It is a network service to determine a user's identity.
- **v) Non-repudiation***:* It ensures that the information originator cannot deny having sent the message.

1.4 Attacks against a multicast communication:

An adversary may carry out both passive and active attacks against a multicast communication, such as:

- *i)* Snooping on confidential communication: - Unauthorized accessing of other's data i.e. to pry or enquire information which is private.
- *ii)* Information disclosure: - To leak or reveal the data which is kept in secret.
- *iii)* Impersonation (masquerading or spoofing): - Pretending to be another person that he's not and accessing the data illicitly.
- *iv)* Modification or fabrication: - Changing or altering the portion of legitimate data with inappropriate one.
- *v)* Replay of packets: - To retransmit the legal data in order to trick the receiver for false identification or duplicate transmissions.
- *vi)* Disrupting a group session: - To interrupt or disturb the session drastically by discontinuing the communication network.
- *vii)* Obstructing data transmission:- To block the data transfer deliberately and make it difficult for other party to communicate.
- *viii)* Introducing false data traffic: - To present the illegal data within the valid data and send it to the receiver.
- *ix)* Camouflage to join a group session: - To conceal or disguise others to join a session without authentication.

x) Commencing a spurious group session: - To initiate a fake or false session by enticing others to join.

xi) Scheming the group members: - To trick the valid users to exchange information in order to gain unauthorized access to data which may contain cryptographic key and other group related information.

1.5 Peer- to- Peer networking:

Secure group communication infrastructure supports a dynamic and scalable Peer- to- Peer model. Applications like file sharing, online gaming, audio/video conferencing, virtual meeting and discussion forums are examples of systems which are organized as peer group. Peer group framework provides flexible structure to communicate and share etc. A Peer-to-Peer model inherently makes these applications easier to design and to operate for groups. In P2P network, all peers (workstations) will have equal priority and responsibility. A peer acts as both client and server. Client/server architecture is purely different and opposite to P2P.

The main important goal in P2P networks is that all clients provide resources, including bandwidth, storage space, and computing power. They have decentralized control thus they avoid single point failure. Due to this they can resist to intentional DOS (Denial of Service) attacks. P2P network has a number of benefits over the traditional client-server model in terms of efficiency and fault-tolerance, surplus security threats. P2P Networks are classified into two types:

i) **Pure P2P networks:**All participating peers are equal, and each peer plays both the role of client and server. The system does not rely on a central server to help control, coordinate, or manage the exchanges among the peers.
Ex:Gnutella, Freenet.

ii) **Hybrid P2P networks:** A central server exists to perform certain Administrative functions to facilitate P2P services.
Ex: Napster

Advantages of P2P Networks:

i) They improve scalability by avoiding dependency on centralized points.
ii) A P2P network is easier to set up, so it's implementation time and cost is less.
iii) It eliminates the need for costly infrastructure by enabling direct communication among clients.
iv) It enables resource aggregation.

Table 1. Features of P2P Networks

Features	**Description**
Secure	Robustness if there are failures or directed attacks
Scalable	Scalability from simple LANs to the entire Internet
Server less	No central point of failure
Self-tuning	Adapts to changes within the infrastructure
Self-repairing	Automatically repairs and corrects itself
Sharing	Enables sharing from edge-of-network endpoints

II. RELATED WORK

Network security is a stimulating problem created due to the intricacy of underlying hardware, software, and network interdependencies by human as well as social factors. It involves decision making in multiple levels and time scales, with prearranged limited resources available to both malicious attackers and administrators defending the networked systems. The resources can vary in bandwidth, computing, and energy at the machine level to manpower and scheduling at the organizational level. Due to this, there is a lot of research proceeding in the field of mapping information security events to mathematical models to moderate risks and threats.The role of Mathematics in a complex system such as the Internet has yet to be extremely explored and researched. Mathematics has been immensely used in physics and many other fields. It has also been widely and efficiently used tool in security to analyze a large amount of network data and simulating the models.

2.1 Methods:

Mathematics can be used in diverse fields of security:-

1) TRANSPORTATION AND BORDER SECURITY
   - i) Machine-assisted Baggage searches - *Pattern recognition*
   - *ii)* Border security - *decision support software*
   - iii) Statistical analysis ofFlight/aircraft inspections - *Statistics*
   - iv) Port-of-entry inspection Algorithms - *Statistics and combinatorial Optimization*
   - v) Vessel tracking for homeland defense - *geometry and calculus*

2) COMMUNICATION SECURITY
   - i) Resource-efficient security protocols for providing data confidentiality and authentication in cellular, ad hoc, and wireless local area networks - *Number theory (Cryptography)*
   - ii) Exploiting analogies between computer viruses and biological viruses - *Differential equations, dynamical Systems*
   - iii) Information privacy i) Identity theft and ii) Privacy of health care data - *Number theory (cryptography), Statistics*
   - iv) Using economic weapons to protect against agro terrorism - *Game Theory Optimization*

3) SURVEILLANCE/DETECTION
   - i) Detecting a bioterrorist attack using syndromic surveillance - *Statistics, Discrete Math*
   - ii) Weapons detection and identification (dirty bombs, plastic explosives) - *Linear algebra, Statistics*
   - iii) Biometrics
     - a) Face, gait, voice, iris recognition
     - b) Non-verbal behavior detection (lying or telling the truth?) (applications to interrogation) - *Optimization, linear algebra, statistics*

4) RESPONDING TO AN ATTACK
   Exposure / Toxicology: a) Modeling dose received and b) Rapid risk and exposure Characterization - *Differentia Equations, Probability*
   - i) Simulating evacuation of complex Transportation facilities - Computer simulation
   - ii) Emergency Communications
   - a) Rapid networking at emergency locations
   - b) Rapid tele collaboration - *discrete math, network analysis.*

III. PROPOSED WORK

3.1 What is Keller box method:

In this paper, we propose a method called ***"Keller Box method"*** which is the implicit two -point finite difference approach, introduced by H. B Keller in 1970's and subsequently it is exposed by T. Cebeci. This numerical scheme is effectively used to solve various boundary layer problems under different geometrics. To solve the non-linear parabolic partial differential equations, Keller box method is efficiently used.

Basic concept: $\frac{\partial f}{\partial t} = \alpha \frac{\partial^2 f}{\partial x^2}$

Define: $u = f;\ v = \frac{\partial f}{\partial x}$ $[f^{1} = u\ ;\ u^{1} = v]$

Yielding: $\frac{\partial u}{\partial x} = v$ $[v = u_x]$

$\frac{\partial u}{\partial t} = \alpha \frac{\partial v}{\partial x}$ $[u_t = \alpha v_x]$

Where *u*, *v* are parameters.

3.2 Definition of mathematical symbols used:

1) **Function (f):**A Function is a relation between set of inputs and a set of permissible outputs. i.e. *f* takes an input *x*, and returns a single output *f* (*x*).

Specification:
A Function can be used in:-
i) Graphs, ii) Derivatives and Equations, iii) Formulas and Algorithms and iv) Computability

2) **Partial derivative (∂):** A derivative of a function of two or more variables with respect to one variable, the other(s) being defined as constant.

Specification:
A partial derivative can be used in:-
i) Vector Calculus, ii) Differential Geometry, iii) Optimization problems, iv) First order derivations, v) Second order derivations as partial and mixed, vii) Higher order derivations as partial and mixed and viii) Statistical Mechanics

3) **Alpha (α):** It is the 1st and lowercase Greek letter.

Specification:
An Alpha can be used in:-
i) Algebraic solutions as Angles, ii) Statistics and Lambda Calculus, iii) Physics and Organic Chemistry and Science and Electronics

4) **Delta (δ):**It is the 4th and lowercase Greek letter.

Specification:
A Delta can be used in:
i) Calculus and Statistics
ii) Automata and Engineering Mathematics
iii) Physics, Chemistry and Astronomy

5) **Theta (θ):** It is the 8th and lowercase Greek letter.

Specification:
A Theta can be used in:
i) Geometry and Number Theory
ii) Physics and Thermodynamics
iii) Meteorology and Population Genetics.

6) **Phi:** It is the 21st uppercase(*ϕ*)and lowercase(*φ*)Greek letter.

Specification: A lowercase Phi can be used in: i) Algebra, Set and Number Theory, ii) Probability Theory and iii) Solid - State Physics , Thermodynamics and Organic Chemistry
An uppercase Phi can be used in: Normal Distribution in Statistics and ii) Vector Calculus and Physics

3.3 How Keller box method is used based on first order derivatives:

1) **First Order Derivative**: A Differential Equation is an equation with a function and one or more of its derivatives.

Ex: An equation with the function y and its derivative (differential) $\frac{\partial y}{\partial x} = y + \frac{\partial y}{\partial x} = 5x$

There are four steps in Keller box method:

First. The complex non - linear differential (momentum) equations are written in First - order derivatives satisfying the Boundary layer conditions.

The Boundary layer conditions are :

$$f(\varphi, 0) = 0, f'(\varphi, 0) = 0, \theta(\varphi, 0) = 1$$
$$f'(\varphi, \infty) = 0, h(\varphi, \infty) = 0, \theta(\varphi, \infty) = 0$$

Second. Write the difference equations using central differences by substituting new independent parameters *u(x,n) , v(x,n) , p(x,n) and q(x,n)* .

When substituting these initial parameters,

$$f' = u\ ; u' = v; \theta' = p;\ \ h' = q \text{ and } q' = p$$

Then the corresponding boundary conditions take the form,

$$f(0,\varphi) = u(0, \varphi) = 0, \theta(0, \varphi) = 1\ ;\ \ u(\infty, \varphi) \to 0, \theta(\infty, \varphi) \to 0$$

After using central differences, the associated boundary conditions are,

$$Y1 = 0 : U1,k = V1,k = 0, \theta 1,k = 1;\ YL \to \infty : UL,k \to 0, \Phi L,k \to 0, \theta L \text{ and } k \to 0$$

Where subscripts k and i are used to represent X and respectively.
By using these resultant conditions, accuracy of a problem can be achieved.

3.4 Advantages of Keller box method

Keller Box Scheme has lot of advantages when used for various applications in Mathematics and Physics:-

i) This scheme is implicit with second order accuracy in both space and time and allows the step size of time and space to be arbitrary (non uniform).
ii) It is efficient and appropriate for the solution of parabolic partial differential equations.
iii) The accuracy of the Box Method has been studied for incompressible and compressible, laminar and turbulent boundary layers past two-dimensional and axisymmetric bodies.
iv) The Efficiency, Speed, and Accuracy of this three dimensional numerical method with the turbulence models for the Reynolds stresses, can be calculated.
v) This method was developed and used to solve one dimensional time fractional diffusion equations.

IV. PROPOSED WORK

The following assumptions are considered for the proposed system:
i) Peers have equal computational Keller box 1st or 2nd order.

ii) There are no privileged, centralized, or trusted peers to manage trust relationships using Keller box output.
iii) Peers occasionally leave and join the network.
iv) A peer provides services and uses services of other
v) For simplicity of discussion, one type of interactions considered in the service context, i.e., file download

METODOLOGY:

Step 1: When the sender wants to send the massage that should be calculated with Keller box encrypted with secret key that is symmetric encryption.

Step 2: The receiver's also use Keller Box for secret key which can be shared by both sender and receiver.

Step 3: Both encrypted message and encrypted key are packed in a single packet, to protect our data we are using the Digital Envelope, which is to be sent to the receiver.

Step 4: At the receiver side (no need to use symmetric key encryption, can use symmetric encryption for the secret key transmission) decryption will be performed to get the original message

V. FUTURE WORK

While this research provides a useful contribution in understanding the secure group communication and Keller box method, there is a plenty of scope for further analysis in this subject.

Third : Linearize the resulting algebraic equations by Newton's method and write them in the Matrix – vector form. Then the boundary conditions become,

$$\delta f_0 = \delta u_0 = 0,\ \delta\theta_0 = 1;\ \ \delta u_J = 0,\ \delta\theta_J = 0$$

Fourth: Solve the Linear system of equations by the Block Tri – diagonal Elimination technique. In order to eliminate the lowest diagonal term which results in an upper bi-diagonal form of the equations, Gauss elimination method is used. After using elimination technique, associated boundary conditions are,

$$Y = 0 : U = V = 0,\ \theta = 1;\ Y \rightarrow \infty : U \rightarrow 0,\ \Phi \rightarrow 0,\ \theta \rightarrow 0$$

These are the two final steps in which the work covered in this research, can be further extended.

VI. EXAMPLES

Some examples are listed of how a mathematical method can be implemented in network security.

Table :: Mathematical Methods Used In Security

Mathematical Methods	**Used in Network Security**
Statistics	Traffic engineering, Multimedia
Stochasticanalysis	QoS, Multicast
Markovchains	Wireless, Sensors
Queueingtheory	Traffic engineering , TCP, Wireless, Sensors, Switches
Scheduling	Sensors, Switches, Mobility
(non)Linear Programming	Traffic engineering , Wireless, Routing
Gametheory	Traffic engineering , TCP, Routing
Control theory	Security, Multimedia
Differential equations	P2P, Security

Coding theory	Multicast, Routing
Graphtheory	Routing, Sensors
Logic	BGP, Routing

VII. CONCLUSION

In this paper, we have recommended this numerical scheme as it can be applied to complex problems having physical measures and easy to cover the impact of variable properties. This method has been so accurate as it is used for both compressible and incompressible, laminar and turbulent boundary layers for 1-D, 2-D, 3-D and axisymmetric bodies. Hence this numerical procedure derives out to be the most suitable technique and ultimately tends to exceed the probable final solution.

VIII. ACKNOWLEDGEMENT

We, the authors wish to thank all the anonymous readers and referees for their resourceful comments

REFERENCES

[1] Abdullah Abdullah, F. a. (2012). The Implicit Keller Box method for the one dimensional time fractional diffusion equation, *2*(3), 69–84.
[2] B. Courbet, J.-P. Croisille, Finite volume box-schemes on triangular meshes. Math. Model. Numer. Anal. 32, 631-649, 1998.
[3] J.-P. Croisille, Finite volume box-schemes and mixed methods. Math. Model. Numer. Anal. 34, 1087-1106, 2000.
[4] Alias, N., Hamzah, N., Amin, N. S., Darwis, R., Satam, N., &Ghaffar, Z. S. A. (2010). Parallelization of iterative and direct schemes for keller-box method on distributed memory platform. In *ICCET 2010 - 2010 International Conference on Computer Engineering and Technology, Proceedings* (Vol. 2). doi:10.1109/ICCET.2010.5485561
[5] J.-P. Croisille, I. Greff, An efficient box-scheme for convection-diffusion equations with sharp contrast in the diffusion coefficients. Computers and Fluids 34, 461-489, 2005.
[6] J.-J. Chattot, A conservative box-scheme for the Euler Equations. Int. J. Numer. Meth. Fluids 31, 149-158, 1999.
[7] Appendix A Keller-Box Method. (n.d.), 201–232.
[8] Chowdary, K. M. K., &Sahu, P. K. (2012). Secure Group Communication Based Encoding Mechanism, 287–291.
[9] Esfahanian, V., &Torabi, F. (2006). Numerical simulation of lead-acid batteries using Keller-Box method. *Journal of Power Sources*, *158*, 949–952. doi:10.1016/j.jpowsour.2005.11.031
[10] Kiah, L. M. (2007). A Key Management Framework for Secure Group Communication in Wireless Mobile Environments. *Doctor of Philosophy, Department of Mathematics*, …, (May 2007). Retrieved from http://digirep.rhul.ac.uk/items/b929b5ef-99d5-44f9-9b6b-700c60b65b55/1/
[11] H. B. Keller, A new difference scheme for parabolic problems, Num. Solns. of Partial Differential Equations, II (Hubbard, B. ed.)., 327-350. New York: Academic Press, 1971.
[12] Meza, J., Campbell, S., & Bailey, D. (2009). LBNL Mathematical and Statistical Opportunities in Cyber Security, 1–11. Retrieved from https://hpcrd.lbl.gov/~meza/papers/CyberMath.pdf
[13] Nadu, T. (2009). STUDY OF DIFFERENT ATTACKS ON MULTICAST.
[14] Perot, J. B., & Subramanian, V. (2007). A discrete calculus analysis of the Keller Box scheme and a generalization of the method to arbitrary meshes. *Journal of Computational Physics*, *226*, 494–508. doi:10.1016/j.jcp.2007.04.015
[15] Project, B. T. (2007). Secure Group Communication.
[16] Rayi, S., &Madhuri, N. (2013). A Secure Group Communication Using Mod-Encoder Compression Algorithm, (2), 120–124.
[17] Sarif, N. M., Salleh, M. Z., &Nazar, R. (2013). Numerical solution of flow and heat transfer over a stretching sheet with newtonian heating using the keller box method. In *Procedia Engineering* (Vol. 53, pp. 542–554). doi:10.1016/j.proeng.2013.02.070
[18] T. Cebeci, K. C. Chang and P. Bradshaw, Solution of a hyperbolic system of turbulence model equations by the "box" scheme. Computer Methods in Appl. Mech. and Engg. 22, 213, 1980.
[19] P. Bradshaw, T. Cebeci and J. H. Whitelaw, Engineering Calculation Methods for Turbulent Flow, Academic Press, 1981.
[20] J.-P. Croisille, Keller's box-scheme for the one-dimensional stationary convection-diffusion equation. Computing 68, 1, 37-63, 2002.
[21] Congress, W., Kechil, A., & Let, M. F. (2011). Unsteady MHD Laminar Boundary Layer Flow due to an Impulsively Stretching Surface, I(January), 6–9.
[22] J.-J. Chattot, Box-schemes for first order partial differential equations. Adv. Comp. Fluid Dynamics, pp. 307-331. New York: Gordon Breach Publ., 1995.

[23] Scholar, M. T., &Dapartment, C. (2014). A Mod-Encoder Compression Algorithm for Secure Communication, *7782*, 70–76.
[24] Simon, S. (1991). Peer-to-peer network management in an IBM SNA network. *IEEE Network*, *5*(February), 30–34. doi:10.1109/65.75839
[25] Wang, Y. (2008). Key Management for Secure Group Applications in Wireless Networks.
[26] Wolthusen,S.D.(n.d.).The_Role_Of_Mathematics_In_Science.pdf.
[27] Wong, C., Gouda, M., & Lam, S. S. (2000). Secure group communications using key graphs. *Networking, IEEE/ACM …*, *8*(1), 16–30. doi:10.1109/90.836475
[28] Yang, Y. R., Lam, S. S. S., Abdullah, F. a, Kiah, L. M., Chowdary, K. M. K., Sahu, P. K., … Project, B. T. (2007). Secure Group Communication. *Doctor of Philosophy, Department of Mathematics, …*,*8*(3), 70–76. doi:10.1109/90.836475.

Dr. Koduganti VentakaRao is working as Professor of CSE and DEAN – IQAC - Vignan's Institute of Information Technology, Visakhapatnam. He has experience for over 22 years in teaching field. He has published 31 papers in his area of expertise. His areas of interest are Security and Cryptography, Parallel Computing and Grid Computing.

S V P K SatyaDev is working as Assistant professor in the Dept of CSE, vignan institute of information technology, Visakhapatnam. He is having over 12 years of teaching experience, his area of interest includes software quality, algorithm analysis and cryptography. Presently pursuing PhD in Andhra University-Visakhapatnam-AP.