International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 21 Issue 2 – APRIL 2016.

A NOVEL CERTIFICATE AUTHENTICATION & VERIFICATION SCHEME FOR RISKAWARE IN MANET

N.Dhineshkumar[#1], K.Manibharathi*[2], R.Ganesh[**3], M.Mayamoorthi[***4]

[#]*B.Tech, Department of Electronics and Communication Engineering Achariya College of Engineering Technology Pondicherry, India*

[*] *B.Tech, Department of Electronics and Communication Engineering Achariya College of Engineering Technology Pondicherry, India*

[**] *B.Tech, Department of Electronics and Communication Engineering Achariya College of Engineering Technology Pondicherry, India*

[***] *B.Tech,Department of Electronics and Communication Engineering Achariya College of Engineering Technology Pondicherry, India*

dhineshkumar858@yahoo.com
evanbharathi@gmail.com
ganiganesh@gmail.com
mayamoorthi94@gmail.com

***Abstract*--The MANET being an emerging open network interconnection, often is exposed to threats present in and out of the network. The existing SIEVE method incorporates the ranking method integrated with the belief probability to check for the node consistency. The process is initiated from an autonomous graph construction of each nodes followed by error check at each edges. The chunk by chunk inspection method fails when the entire throughput is not transferred to the maximum level or in handling network load. The overall performance degrades when the un-trusted nodes in a network increases. The chance for trusted and un-trusted is neither differentiated for the path selecting process. To reform the shortcomings of the network, Trust based Forwarding Propagation (TFP) is proposed which abides the verified nodes for transmission. The trusted and non-trusted nodes are managed under a list from which each transmission is initiated. Location based neighbour detection improves the chances of mismatching probability in selecting fault nodes for transmission. This improves the network performance in terms of throughput by minimizing misdetection and false positive rate in a network.**

***Keywords*-MANNET; SIEVE; Trust based Forwarding Propagation.**

I. INTRODUCTION

In recent years, the explosive growth of mobile computing devices, which mainly include laptops, personal digital assistants (PDAs) and handheld digital devices, has impelled a revolutionary change in the computing world: computing will not merely rely on the capability provided by the personal computers, and the concept of ubiquitous computing emerges and becomes one of the research hotspots in the computer science society. The nature of the ubiquitous computing has made it necessary to adopt wireless network as the interconnection method: it is not possible for the ubiquitous devices to get wired network link whenever and wherever they need to connect with other ubiquitous devices.

The Mobile Ad Hoc Network is one of the wireless networks that have attracted most concentrations from many researchers. A Mobile Ad hoc Network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. People and vehicles can thus be internetworked in areas without a pre-existing communication infrastructure or when the use of such infrastructure requires wireless extension. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node to communicate with each other. In these two situations, all the nodes that have participated in the communication automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network.

This paper is organized as follows: The Existing system model II, The proposed system model III. In section IV, Result and Discussion are discussed and concluding remarks is given in section V.

II.EXISTING SYSTEM

The SIEVE protocol is based on the ranking method. The nodes that have the maximum decoding capability are

given the highest priority in the network and such nodes are labelled as trust nodes or honest nodes. These nodes will be given the highest ranks. SIEVE method incorporates the ranking method integrated with the belief probability to check for the node consistency. The process is initiated from an autonomous graph construction of each nodes followed by error check at each edges. The chunk by chunk inspection method fails when the entire throughput is not transferred to the maximum level or in handling network load. The overall performance degrades when the un-trusted nodes in a network increases. And also when a malicious node in the network remains inactive there are chances of this SIEVE protocol to count it as a trusted node providing a rank within the network. Thus the malicious node path inclusion probability in the network will increase.

SIEVE uses LT codes decoding mechanism to detect modified chunks and exploits the Belief Propagation (BP) algorithm to identify malicious nodes.

A.LTCode Mechanism

According to the dissemination strategy every node keeps collecting from different up loaders sets of coded blocks corresponding to different chunks. LT codes can be exploited to detect if modified blocks have been collected without the need of any supplementary verification mechanism.

LT codes have been proposed in and represents one of the first embodiment of the class of rateless codes, these are a particular family of erasure codes where the rate is not fixed by design, so that the number of coded packets can be decided and changed on the fly.LT codes are ratelessbased on the binary Galois field GF, i.e., coded packets are computed with simple binary XOR of random sub- sets of the K original data blocks.

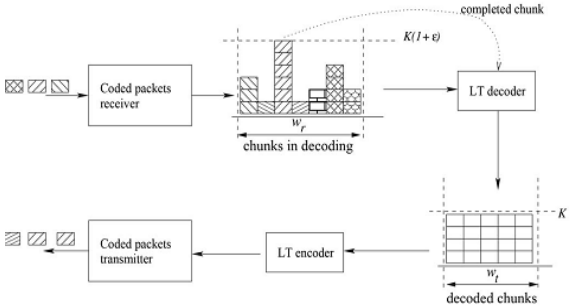

Fig. 1. Node operations: LT encoding, decoding and dissemination protocol.

In it is shown that selecting the number of blocks to be combined, termed as the packet degree d, according to the Robust Soliton Distribution (RSD).

B.Belief Propagation Algorithm

The BP algorithm can be used to estimate from the factor graph the so called variable marginal (P(xi))i∈U,i.e. the probability of node i being malicious. BP is an iterative algorithm based on the exchange of probability estimates (also called messages or beliefs), along the edges of the bipartite graph Gn. In case of a Bayesian network BP represents a closed-form solution for the marginal. Nonetheless, the same algorithm has proven to be a robust estimator for the variable marginal of general factor graph. In our setting it is convenient to distinguish between two classes of messages: message from up-loader to check and message from check to up loader.

The BP algorithm is based on iterative refinements of the check messages based on the current values of the node messages, followed by updating of messages as a function of node pass.

III.PROPOSED SYSTEM

Hence in proposed system we had overcomes the challenges of using SIEVE protocol. The goal of security services in MANETs is to protect information and resources from attacks and misbehaviour. These security services such as privacy, integrity and authentication cannot be achieved without a prior solid key management. The major problem in providing security service in ad hoc networks is how to manage the key that provide trustworthiness and privacy in data communication. Trust is a dynamic phenomenon as it changes with time, experience and the state of different sources based on the environment and mobility. Trust propagation can be of multi hop and is based on the transitivity property of trust.

The core factor to be considered for trust propagation is cooperation in the network for transporting the trust information as shown in Figure. We have proposed a mechanism based on trust propagation to provide trust conscious secure route data communication support in reactive Ad hoc On-demand Distance Vector Routing (AOMDV) protocol.

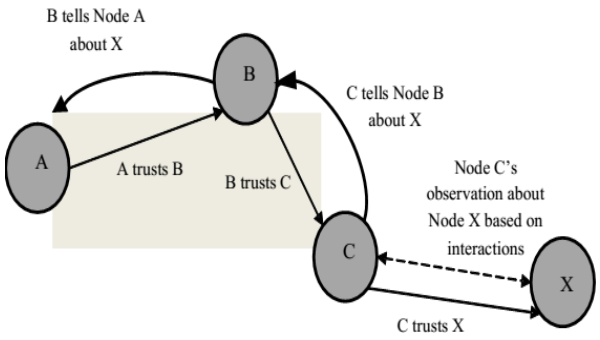

Fig. 2Trust based propagation

A. Trust neighbor Discovery System Model

The initial step in the setting up the Ad Hoc networks is the neighboring discovery. Then after discovering the neighboring the system will monitor the neighboring nodes

by capturing the network packets. The neural network is trained with the past historical data and the weights are adjusted accordingly to get the desired output. Then the gathered packet related information is fed to the trained neural network to compute the trust value.

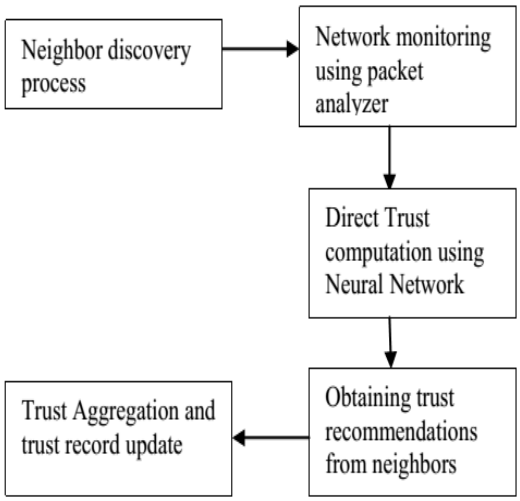

Fig.3 Trust Neighbor Discovery System Model

The algorithm used in the proposed system for ND is Scan based Random algorithm for neighboring discovery. The scam based algorithm used in the proposed system is completely random algorithm (CRA). The CRA does not have the prior knowledge of how many number of nodes are there in the network.

The CRA used in the proposed system is the direct discovery algorithm that uses the directional antenna for transmission and reception of signals. The algorithm requires the nodes to that communicate to be synchronized. The can successfully transmit and receive only if the nodes are in complementary mode. The algorithm divides the time frame into three slots. During the first mini slot the node decides to be in any one of the following state. The states of node are described astransmit, sleep and Listen

When a node chooses to be in transmit mode, it broadcasts the discover message in the first mini-slot and waits for the ACK in the second mini-slot. During third mini slot it sends the confirmation to the receivers. When the node chooses to be in listen mode, it receives the discover message in the second mini-slot and sends the ACK to the sender if it successfully receive the discover message. In the third mini-slot it receives the confirmation message from the sender.

B.Trust Computation Technique

The algorithm used for computing the trust of the neighboring nodes in the proposed system is relationship maturity based distributed trust management scheme. This algorithm used in the proposed system is distributed where every node computes the trust of every other node. It uses both direct trust and recommendation based trust for computing the trust. To perform the weight age of the recommendation the proposed system uses the relationship maturity concept where the age of relationship is measured. The Nodes increase the weight of the recommendations coming from older neighboring and decrease the weight of recommendations coming from new neighboring.

IV.SIMULATION RESULTS

A. Data Transfer between Source & Destination

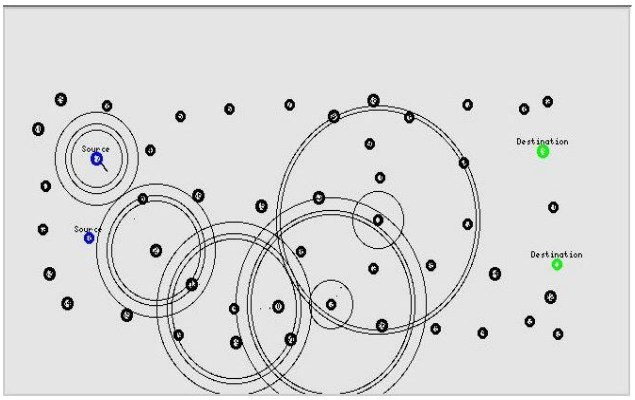

Fig 4a Communication between nodes in Mobile Adhoc networks

Based on the decoding capability of each and every nodes in the network, the SIEVE assigns rank to the highest priority nodes. Initially in this network the source is communicating with the destination. In this scenario the malicious nodes in the network are inactive for a particular period of time. The source here is the blue coloured node and the destination is the green coloured node

B.Malicious Nodes in the Network

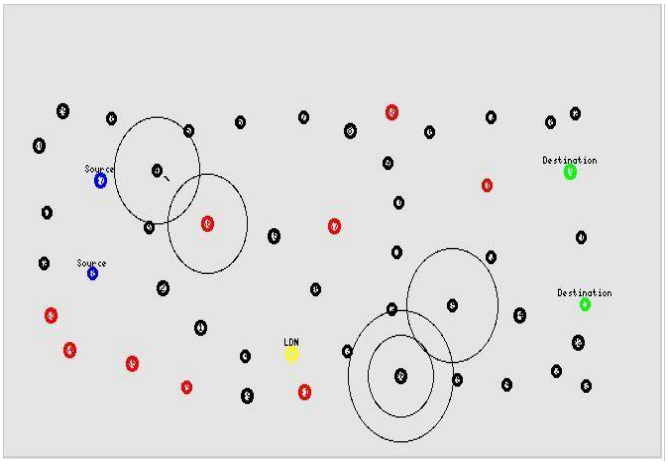

Fig: 4b Communication between malicious nodes

As the time increases the number of attackers or polluters in the network increases. In this network there are 9 malicious nodes (red coloured nodes) and these nodes take part actively in the network activities. When all the malicious nodes are active in the network it covers even the path between source and destination. So the source is unable to communicate with the destination and it becomes ideal until the malicious nodes are active.

D.Communication through Link Nodes

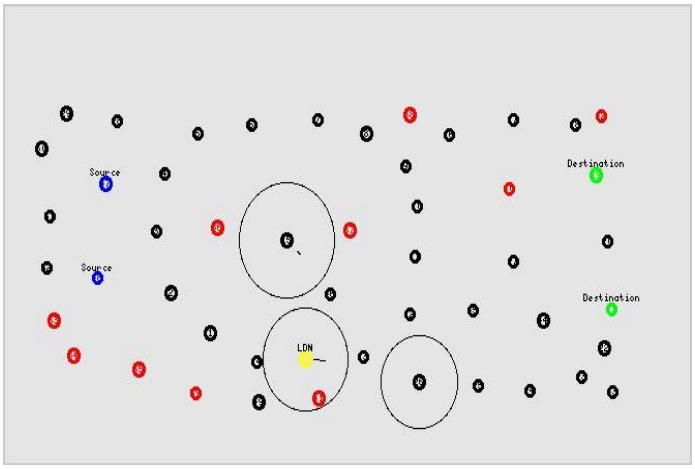

Fig: 4c Communication through link nodes

Here the source and destination communication is through the link nodes. Link nodes (yellow coloured nodes)are the nodes that will be always in communication with the destination and also with other link nodes in the network. So the source finds the link node that is near to it and passes the data that is to be sent to the destination. The link nodes are also reliable nodes that are defined by the network itself. So the data will be transferred to the destination via link nodes without any information loss. The SIEVE protocol will create the link node to transfer the data secure. The algorithm generate the LDR link node, they assign LDR as a secure node to transfer the data.

C. Performance of Sieve Protocol

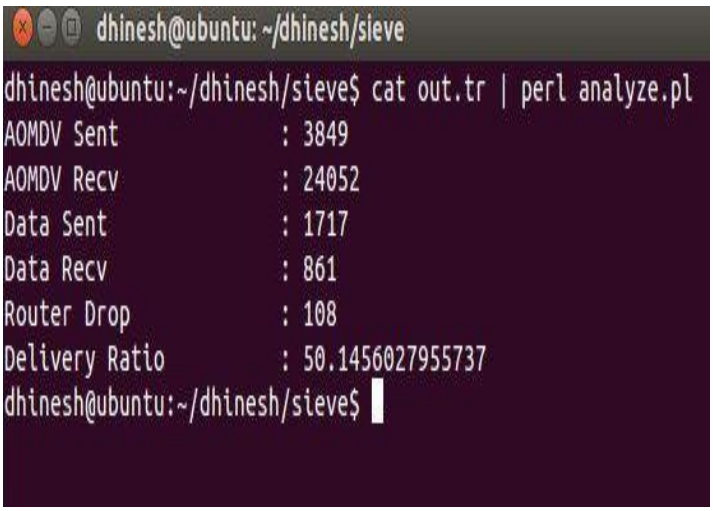

Fig 4c Performance of SIEVE Protocol

The above figure shows the overall performance of the network when the SIEVE i.e.ranking method is implemented. The overall performance includes the total number of packets sent, total number of packets received, and drop of packets, delivery.

D. Performance of Sequential Routing Protocol

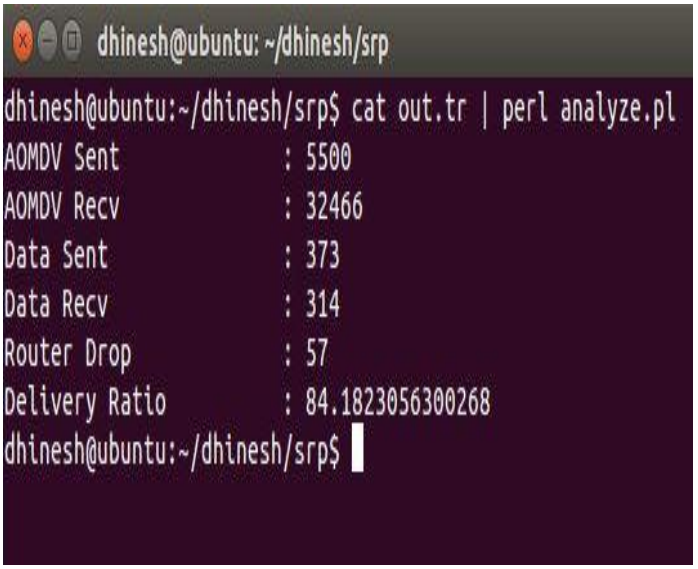

Fig 4d Network performance of sequential routing protocol

The above figure shows the overall performance of the network when the Trust based forwarding propagation is implemented. The overall performance includes the total number of packets sent, total number of packets received, and drop of packets, delivery ratio. Implementation of the Trust based forwarding propagationincreases the delivery ratio and throughput by an approximation of 34% when compared to the existing rank method.

E.Transmission of Data Via Secure Nodes

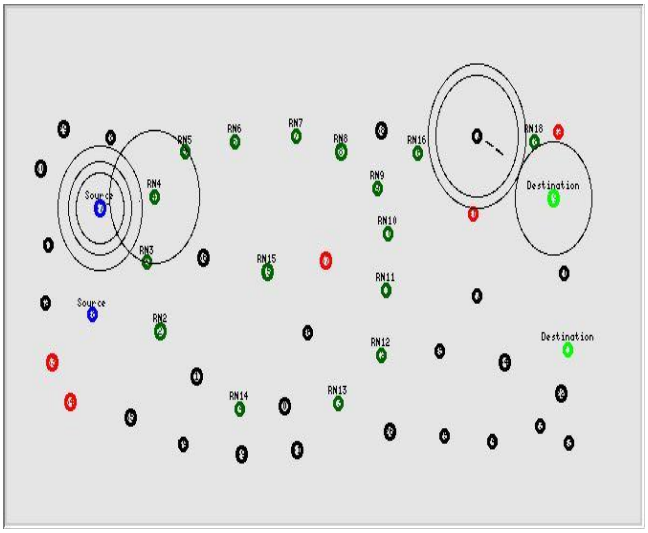

Fig 4e Transmission of Data via Secure Nodes

The above figure shows the transmission data via secure nodes when the Trust based forwarding propagation is being deployed. The secure nodes that are identified by the network. Initially the node location is broadcasted. Then for each transmission the distance is being checked every time. If the saved distance and the checking distance is the same, then that node is identified as a secured node and data will be given to that node accompanied by a private key. If the distances are not the same the connection will be terminated and rebroadcast occurs.

F.Throughput

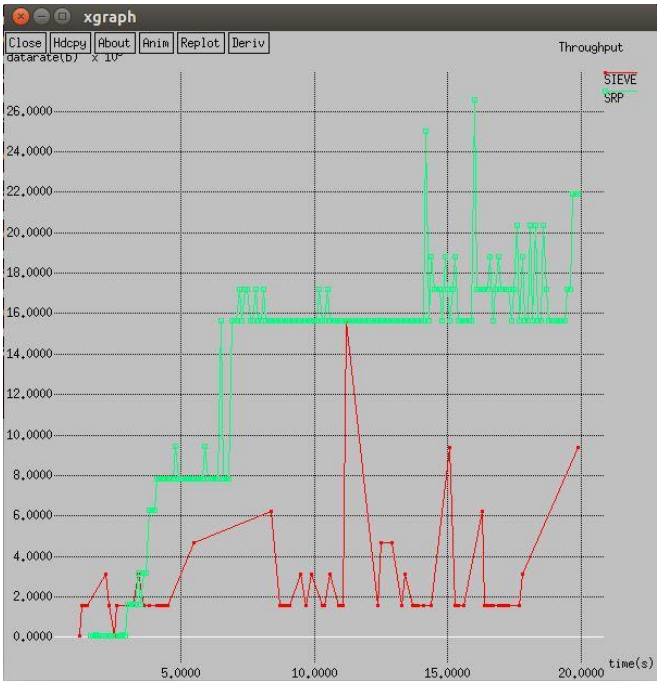

Fig*: 4f Throughput*

G .Misdetection

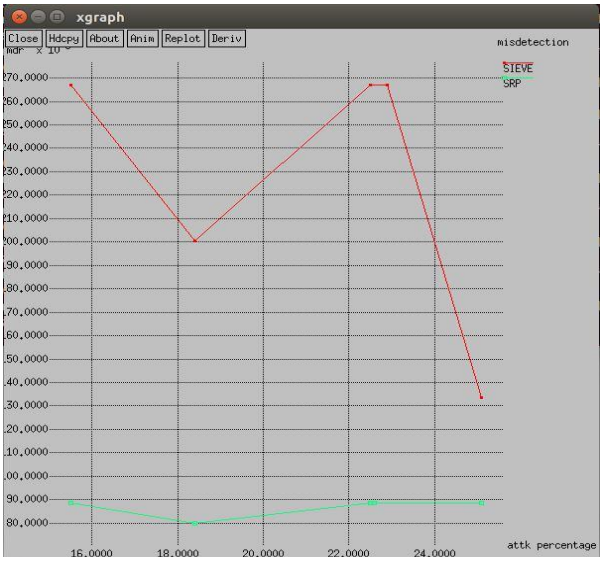

Fig:4g Misdetection

H.Drop

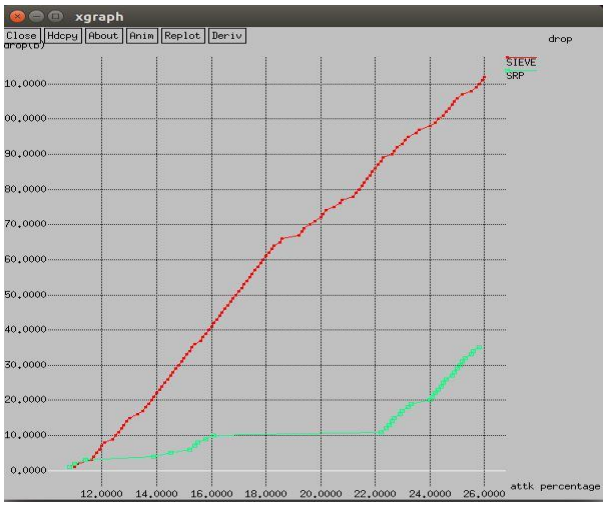

Fig 4h Drop

J .False rate

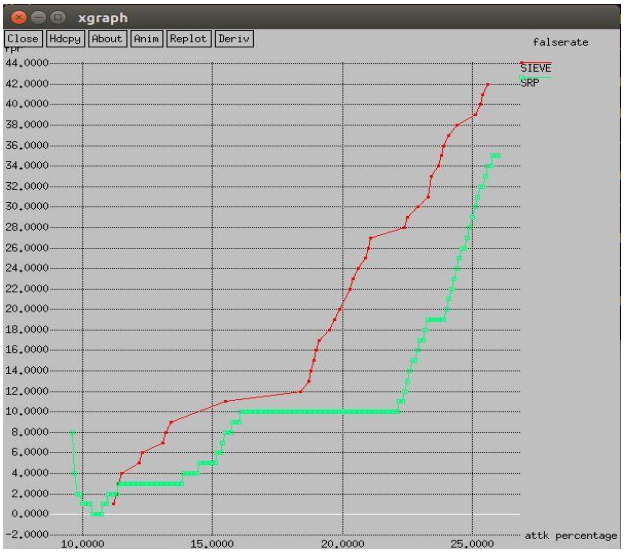

Fig 4j .False rate

V.CONCLUSION AND FUTURE SCOPE

A. Conclusion

The SIEVE method is incorporated based on ranking method integrated with the belief probability to check for the node consistency. The process is initiated from an autonomous graph construction of each nodes followed by error check at each edges. The chunk by chunk inspection method fails when the entire throughput is not transferred to the maximum level or in handling network load. The overall performance degrades when the un-trusted nodes in a network increases. When a malicious node is inactive in the network the SIEVE might take it as a trusted node providing a rank within the network. Thus the malicious path inclusion probability in the network is increased.

To reform the shortcomings of the network, trust based forwarding propagation (TFP)architecture is proposed to ensure seamless communication. The communicating terminal can make use of link node structure to provide un-interrupting links to the destination. This ensures reliability in terms of network load and throughput. However achieving the link node communication at the first broadcast is either 1 or 0. If it is the condition then we have to apply rank method in the intermediate nodes. Besides all these considerations Trust based forwarding propagation architecture yields a better throughput and delivery ratio.

The proposed trust based forwarding propagationalgorithm improves the network parameters through discern the secure node at each and every broadcast to transmit the data securely.By implementing trust based forwarding propagation architecture will increases the delivery ratio by an approximation of 34% when compared to existing SIEVE method. The network throughput is also gradually increased by about 20% even in an unsecured open system interconnection. The enhanced DR by a ratio of 34%it proves that TFP is best in terms of delivery ratiowhen compared to existing SIEVE method.

B.Future scope

The process can further be extended into Location Aware Routing process at the time of broadcast and opportunistic route selection technique. The protocol limit thesearch for a route, it determined based on the expected location of the destination node at the time of route discovery. It minimizes the overhead and when added with LADR, it can improve the network performance in terms of security and neighbouring discovery.

REFERENCES

[1] Rossano Gaeta, Marco Grangetto, "Exploiting ratelesscodesandbelief propagation to infer identity of polluters inMANET",*IEEE Trans. Inf. Theory, vol. 13, no. 7, pp. 1482-1494, Jul. 2014.*

[2] B. Wu, J. Chen, J. Wu, and M. Cardei, "A survey of attacks andcountermeasures in mobile ad hoc networks," in *Wireless NetworkSecurity*, Y. Xiao, X. S. Shen, and D.-Z. Du, Eds. New York, NY,USA: Springer, pp. 103–134 Apr. 2007.

[3] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile adhoc networks: Challenges and solutions," *IEEE Wireless Commun.*,vol. 11, no. 1, pp. 38–47, Feb. 2004.

[4] J. Pearl, *Probabilistic Reasoning in Intelligent Systems: Networks ofPlausible Inference*. San Francisco, CA, USA: Morgan KaufmannPublishers, Inc., 1988.

[5] D. MacKay, *Information Theory, Inference and Learning Algorithms*.Cambridge, U.K.: Cambridge University Press, Nov. 2003.

[6] J. Yedidia, W. Freeman, and Y. Weiss, "Constructing free-energyapproximations and generalized belief propagation algorithms,"*IEEE Trans. Inf. Theory*, vol. 41, no. 7, pp. 2282–2312, Jul. 2004.

[7] J. Yedidia, W. Freeman, and Y. Weiss, "Understanding belief propagationand its generalizations," in *Exploring Artificial Intelligencein the New Millennium*, San Francisco, CA, USA: Elsevier, Jan. 2003.

[8] T. Schierl, S. Johansen, A. Perkis, and T. Wiegand, "Ratelessscalablevideo coding for overlay multisource streaming in manets,"*J. Vis. Commun. Image Represent.*, vol. 19, no. 8, pp. 400–407 Feb, 2008.

[9] V. R. Syrotiuk, C. J. Colbourn, and S. Yellamraju, "Ratelessforward error correction for topology-transparent scheduling,"*IEEE/ACM Trans. Netw.*, vol. 14, no. 2, pp. 444–472, Apr. 2008.

[10] S. Agrawal and D. Boneh, "Homomorphic MACs: MAC-basedintegrity for network coding," in *Applied Cryptography and NetworkSecurity*. Berlin, Germany: Springer, pp. 292–304, Mar, 2009.

[11] J. Dong, R. Curtmola, and C. Nita-Rotaru, "Practical defencesagainst pollution attacks in intra-flow network coding for wirelessmesh networks," in *Proc. 2nd ACM Conf. WiSec*, Zurich,Switzerland, pp. 111–122, Jul. 2009.

[12] Y. Li, H. Yao, M. Chen, S. Jaggi, and A. Rosen, "Ripple authenticationfor network coding," in *Proc. IEEE INFOCOM*, San Diego,CA, USA, pp. 1–9,Mar. 2010.

[13] A. Newell and C. Nita-Rotaru, "Split null keys: A null space baseddefense for pollution attacks in wireless network coding," in *Proc.9th IEEE SECON*, Seoul, Korea, pp. 479–487,Nov. 2012.

[14] Q. Wang, L. Vu, K. Nahrstedt, and H. Khurana, "MIS: Maliciousnodes identification scheme in network-coding-based peer-topeerstreaming," in *Proc. IEEE INFOCOM*, San Diego, CA, USA, pp. 1–4,Mar. 2010.

[15] R. Gaeta, M. Grangetto, and R. Loti, "SIEVE: A distributed, accurate,and robust technique to identify malicious nodes in datadissemination on manet," in *Proc. IEEE ICPADS*, Washington, DC,USA, 2012, pp. 331–338.

[16] M. Luby, "LT codes," in *Proc. 43rd FOCS*, Washington, DC, USA,2002, pp. 271–280.

[17] R. Gallager, *Low-Density Parity-Check Codes*. Cambridge, U.K.:MIT Press, 1943.

[18] W. T. Freeman, E. C. Pasztor, and O. T. Carmichael, "Learninglow-level vision," *Int. J. Comput. Vis.*, vol. 40, no. 1, pp. 24–47,2000.

[19] M. Luby, M. Mitzenmacher, M. Shokrollahi, and D. Spielman,"Improved low-density parity-check codes using

irregulargraphs," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 484 – 498, Feb.2001.

[20] G. F. Riley and T. R. Henderson, "The NS-3 network simulator,"in*Modeling and Tools for Network Simulation*. Berlin, Germany:Springer, 2010, pp. 14–34.

[21] M. N. Krohn, M. J. Freedman, and D. Mazieres, "On-the-fly verificationofrateless erasure codes for efficient content distribution,"in*Proc. IEEE Symp. Security Privacy*, 2004.

[22] C. Gkantsidis and P. Rodriguez, "Cooperative security fornetwork coding file distribution," in *Proc. IEEE INFOCOM*,Barcelona, Spain, 2004.

[23] Q. Li, D.-M. Chiu, and J. Lui, "On the practical and security issuesof batch content distribution via network coding," in *Proc. 14thIEEE ICNP*, Washington, DC, USA, 2004.

[24] D. Kamal, D. Charles, K. Jain, and K. Lauter, "Signatures fornetwork coding," in *Proc. 40th Annu. Conf. Inform. Sci. Syst.*,Princeton, NJ, USA, 2004.

[25] Z. Yu, Y. Wei, B. Ramkumar, and Y. Guan, "An efficient signaturebasedscheme for securing network coding against pollutionattacks," in *Proc. IEEE INFOCOM*, Phoenix, AZ, USA, Nov. 2008.

[26] E. Kehdi and B. Li, "Null keys: Limiting malicious attacks via nullspace properties of network coding," in *Proc. IEEE INFOCOM*, Riode Janeiro, Brazil, Aug. 2009.

[27] Z. Yu, Y.Wei, B. Ramkumar, and Y. Guan, "An efficient scheme forsecuringxor network coding against pollution attacks," in *Proc.IEEE INFOCOM*, Rio de Janeiro, Brazil, 2009.

[28] T. Ho*et al.*, "Byzantine modification detection in multicast networkswith random network coding," *IEEE Trans. Inf. Theory*,vol. 44, no. 4, pp. 2798–2803, Jun. 2008.

[29] S. Jaggi*et al.*, "Resilient network coding in the presence ofbyzantine adversaries," *IEEE Trans. Inf. Theory*, vol. 44, no. 4,pp. 2494–2403, Jun. 2008.

[30] R. Koetter and F. Kschischang, "Coding for errors and erasures inrandom network coding," *IEEE Trans. Inf. Theory*, vol. 44, no. 8,pp. 3479–3491, Aug. 2008.