TWO STEP VERIFICATION USING HAT (HASHING, ANT COLONY, TRACKING THE IP) TO INFER IDENTITY OF POLLUTERS IN MANET

R.Ananthi, J.Jayapradha

Abstract— **Exploitation of rateless codes in MANET for dissemination of data chunks a node is determined. A node is created for coded block of payloads which gives solution to the problems of malicious node identification which implies pollution attack intentionally. Usually when vulnerable data packets intrude networks with malicious coded node which prohibits decoding of the message data appropriately in a network can be termed as pollution attacks. Normally a node creates check for decoding the chunk autonomously. As the pollution attack described in the existing system would not handle rateless codes which is not that much efficient to protect data while transmission. In this paper we proposed a technique that comprises of two step verification that overcomes every existing disadvantage and provides security without any performance loss. First step verification in this technique identifies the possibility of attack like if any abnormality found. In depth verification verifies the system from root which takes place only when any alarm created from first step of verification. In our new technique we achieve high security so that there is no performance loss during data transmission.**

Index Terms— **Rateless codes, MANET, coded node, pollution attack, data transmission.**

I. INTRODUCTION

The Mobile Ad hoc Network (MANET) utilize any wireless medium such as WiFi connection or any satellite transmission and configure them with changing locations. Because of the dynamic nature the MANET connection is not so secure which have challenges and opportunities for achieving security. Wireless medium is shared by open peer to peer architecture which will have resource constraints in a dynamic network topology [1]. MANET in mobile multiple connectivity they protect basic security problem. MANET provides complete security solutions by detecting and preventing any kind of network attacks [2].

Rateless code wields propagation of MANET where nodes are meant to be data chunks. Any node can decode any chunk successfully by integrating enough coded blocks from various other nodes without any coordination between them [3]. The solution for identifying the malicious nodes which infer pollution attack modifies the payload of code before transmission. Rateless code handles rateless codes which is not so efficient for protecting data while transmission.

In older methods a node is created for check to decode a chunk of data which is composed of coded blocks used for decoding the chunk and a flag indicates the corrupted chunk. The integrity in belief propagation which infers the malicious nodes identified with rateless codes [4] [5]. In the before used techniques the data is not completely secured. Even the technique used for securing data is highly cost effective which results in performance loss. The graph generated for defining these techniques is such a tedious process.

At the application level the cryptography related attack where the nodes in depth are corrupted from particular type which is also defined as pollution attack. The attackers are known as polluters where MANET uses data dissemination application which generates nodes disseminated using rateless codes [6] [7] [8]. Data in the node identifiers has been corrupted along with variable length list. Chunks exploit constraints imparts detection of linear channel coding. The malicious node computes the probability to allow each node from algorithm. Nodes in local factor graph uses checks from own decoding operations by neighbor nodes update its nodes.

Wireless network topology with community wide technical wireless access typically consists of stationary wireless router which communicates through multi hop wireless links [9] [10].

***R.Ananthi**, M.E. CSE Krishnasamy College of Engineering and Technology, Affiliated to Anna University (Chennai), S.Kumarapuram, Cuddalore, Tamil Nadu – 607109, India.*

***J.Jayapradha,** Assistant Professor, Krishnasamy College of Engineering and Technology, Affiliated to Anna University (Chennai), S.Kumarapuram, Cuddalore, Tamil Nadu – 607109, India.*

ISSN: 2278 – 1323

In this paper we suggest a technique which involves two step of verification first identifies the possibility of attack and the second set of verification process involves in depth verification from the root level when any alarm created from first step of verification. This paper also explains how we defend pollution attacks using ant colony algorithm and hashing verification techniques which tracks the IP of attackers and block them perpetually.

II. Related Work

The classification and identification of malicious nodes recasts the marginal probabilities in graph estimation which proposes decentralized appropriate solutions based on proposed algorithm [11] [12]. The data dissemination in selected data use case is very popular. It can be used in any multi party application which will have collaborative entities of detecting a malicious node [13]. In opposite to cryptographic based network coding in a meshed wireless networks for tools that checks the integrity which verifies each and every coded block.

The other method infer identity of malicious nodes achieve simple pollution detection [14]. Based on rateless codes data dissemination protocol which attain pollution detection suitable for MANETs.

Scheduling wireless mobile ad hoc networks theoretically with transparent topology contributes practical deployment. They generalize the requirement which schedules the wider solution for matching the network conditions [15]. The other one bounds the expected throughput which assumes the available acknowledgements. The rate less minimum computational overhead for error correcting scheme is inherently unreliable with the wireless medium where channel load delay is contributed towards renewal interest [16].

In another reference of network protocols with increased throughput the network congestion is reduced with low power consumption and high reliability [17] [18]. The output packets produced by the core principle of network coding is mixed with input packets. When the polluter nodes infuse the corrupted packets which cause severe security threat in network coding systems depletes pollution attack.

As these pollution attacks against network decoding incurs high degradation of throughput [19]. Some light weight schemes combines with time based authentication with linear transformations. They propose optimistic scheme which improves system performance with polluted packet passing is very low [20]. The realistic link of quality measurement protocols from previous experimental test bed improves twenty times more systems performance.

Later researches defend from pollution attacks proposes algebraic approach which reduces computational cost on null spaces than the previous pollution defending mechanism in network coding system. Distribution keys for scaling forward nodes for creating new keys requires source for their distribution [21]. In specified large scale peer to peer systems the wireless networks cannot provide secured system. Security constraint imposes small updates for scalable key distribution relies on forward nodes keys on network topology [22]. From the existing defense mechanisms we infer lower communication and computation overhead which does not require any time synchronization [23] [24].

III. Two Step Verification Technique

In the proposed technique we apply verification and detection of pollution attacks using two step which involves major verification and in depth verification technique. In major verification of pollution attacks the server and client relation established which scrutinizes the status of all clients and server system in which the server will authenticate all the transactions made in a controlled manner.

The first major verification step infused in server which keeps track of several security threats from the initial level. Server tracks the problem using ant colony algorithm when it is needed. If any unauthorized attacking source found then it leads to in depth verification which implies hashing verification of data and generates hashing number denotes the attacked nodes.

As the last step it tracks the IP of the attacker and blocks the attacker nodes and eliminates the further pollution attack by the attacker. In the following section we discuss about the ant colony algorithm, hashing technique and tracking of attackers IP which can infer identities of polluters and eliminate attacks completely.

IV. Ant Colony Algorithm Implementation

For network codes which is vulnerable to pollution attacks the server will keeps tracks of all the existing codes and have several levels to scrutinize the intruders for polluted message packets insertion in any medium of network in MANET [25] [26]. There we employs ant colony algorithm which tracks the servers network transmissions from each tower whenever needed.

ISSN: 2278 – 1323

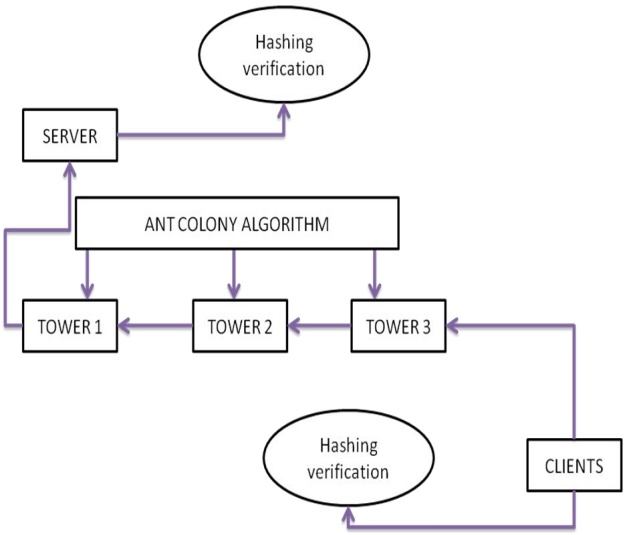

Fig.1 Ant colony algorithm and hashing technique

The ant colony algorithm will scrutinize each and every message packets by leaving text messages in every tower when it passes from one tower to another.

If any intruder detection during scrutinizing the passage of messages from tower to tower they will first find the source network where the intrusion takes place [27]. If the source of intrusion is legitimate and misunderstood to be an intruder then it will redirect the message to the server and starts its normal processing.

If in case of malicious node is detected as a polluter who attempts to attack this can be rechecked by hashing verification done on both sides [28]. When the user starts demanding for data immediately the data will be verified and it generates a number. Thus they once again recheck the attack and confirms in the initial level to enter into in depth level of verification. So they can ensure the security with less time taken but efficiently [29] [30]. As in the ant colony algorithm they leave behind messages such as ants leaves pheromones behind the way they travel. Hence any irregularity found that messages will be re examined for traces of attackers in the messages left in every nodes through ant colony algorithm [31].

The tracking message contains information of the source of the node the messages came from and the destination node which they meant to reach [32]. From Fig.1 we can have a clear idea of how the message from one node to other travels and leave behind the tracking messages in every node. Then the second step verification for suspicious node of pollution attack will be done.

V. IN DEPTH VERIFICATION WITH HASHING TECHNIQUE

Hashing is the second step of malicious node detection in pollution attacks process which involves in depth verification of message nodes. The verification starts from the source where the data starts to bid thus there it generates a number. When data reaches its destination then the admin will verify the data by hashing then it again generates a number. Then both the number generated from the hashing technique will be compared and checked for its unity. If both the number generated is equal then there is no attack. But if any change in the hash number seen then compulsorily some problem exists there which will be verified from the server.

In this verification process which includes various kind of attack checking for messaging nodes will be accurate and mostly appropriate for detecting the attackers promptly. From the first step of verification we can notice that it will not take much time for finding pollution attacks. They analyze most common attack attempts through preliminary steps itself. More than normal attack detection pollution attack detection will be done in less time with prompt action taken.

VI. MEASURES TAKEN FOR IDENTIFIED POLLUTION ATTACK USING HAT

The attack will be detected by the server through two step verification by the server. They implies ant colony algorithm from the first step where the message starts travelling from its source nodes so we have check over the message node in every step of its travel from each node [33]. Then in case of any suspected pollution attack then it undergoes in depth verification which checks for hashing number comparison.

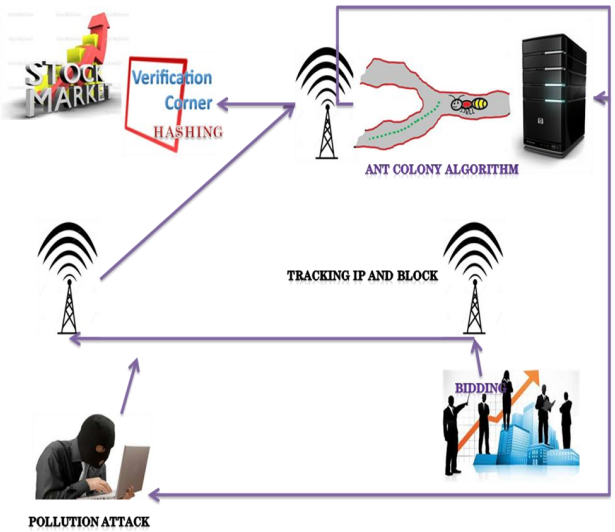

Fig.2 HAT (Hashing, Ant colony and Tracking)

When a substantiated attack is detected then it starts tracking the attackers IP address. The IP address of

ISSN: 2278 – 1323

attacking node will be detected by backtracking and analyzing the ant colony messages then the accurate attacker will be detected. Then the messages sent from detected attackers IP will be destroyed at once and then that IP will be blocked from the network and blacklisted.

From Fig.2 we can infer how the HAT is used for attack detection and prevention. Polluters and their pollution attacks will be ultimately seized and eliminated by the last step taken. This HAT method implied for inferring the identification of polluters will promptly check for pollution attack and thus eliminate attacks instantly.

VII. CONCLUSION

In this paper we explain how the pollution attacks are detected and prevented promptly along with elimination of polluters instantly from the secured network. Attack within MANET includes malicious attack as well as unidentified nodes. The rateless codes in MANETs will be exploited by pollution attacks which is prevented using HAT method. First step with major verification and then in depth verification for attacks and attackers will be précised for ultimate attack detection and prevention. HAT is the two step verification and detection method of attacks using hashing technique and infused ant colony algorithm along with the message transmission. Then they track the IP address of the attacker and then they will be blocked for further attacks.

REFERENCES

[1] B. Wu, J. Chen, J. Wu, and M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc networks," in *Wireless Network Security*, Y. Xiao, X. S. Shen, and D.-Z. Du, Eds. New York, NY, USA: Springer, 2007, pp. 103–135.

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

[3] J. Pearl, *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*. San Francisco, CA, USA: Morgan Kaufmann Publishers, Inc., 1988.

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

[5] J. Yedidia, W. Freeman, and Y. Weiss, "Constructing free-energy approximations and generalized belief propagation algorithms," *IEEE Trans. Inf. Theory*, vol. 51, no. 7, pp. 2282–2312, Jul. 2005.

[6] J. Yedidia, W. Freeman, and Y. Weiss, "Understanding belief prop- agation and its generalizations," in *Exploring Artificial Intelligence in the New Millennium*, San Francisco, CA, USA: Elsevier, 2003.

[7] T. Schierl, S. Johansen, A. Perkis, and T. Wiegand, "Rateless scal-able video coding for overlay multisource streaming in manets," *J. Vis. Commun. Image Represent.*, vol. 19, no. 8, pp. 500–507, 2008.

[8] V. R. Syrotiuk, C. J. Colbourn, and S. Yellamraju, "Rateless forward error correction for topology-transparent scheduling," *IEEE/ACM Trans. Netw.*, vol. 16, no. 2, pp. 464–472, Apr. 2008.

[9] S. Agrawal and D. Boneh, "Homomorphic MACs: MAC-based integrity for network coding," in *Applied Cryptography and Network Security*. Berlin, Germany: Springer, 2009, pp. 292–305.

[10] J. Dong, R. Curtmola, and C. Nita-Rotaru, "Practical defenses against pollution attacks in intra-flow network coding for wire- less mesh networks," in *Proc. 2nd ACM Conf. WiSec*, Zurich, Switzerland, 2009, pp. 111–122.

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

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

[13] Q. Wang, L. Vu, K. Nahrstedt, and H. Khurana, "MIS: Malicious nodes identification scheme in network-coding-based peer-to- peer streaming," in *Proc. IEEE INFOCOM*, San Diego, CA, USA, Mar. 2010, pp. 1–5.

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

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

[16] R. Gallager, *Low-Density Parity-Check Codes*. Cambridge, U.K.: MIT Press, 1963.

[17] W. T. Freeman, E. C. Pasztor, and O. T. Carmichael, "Learning low-level vision," *Int. J. Comput. Vis.*, vol. 40, no. 1, pp. 25–47, 2000.

[18] M. Luby, M. Mitzenmacher, M. Shokrollahi, and D. Spielman, "Improved low-density parity-check codes using irregular graphs," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 585 –598, Feb. 2001.

[19] G. F. Riley and T. R. Henderson, "The NS-3 network simulator," in *Modeling and Tools for Network Simulation*. Berlin, Germany:Springer, 2010, pp. 15–34.

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

[21] C. Gkantsidis and P. Rodriguez, "Cooperative security for network coding file distribution," in *Proc. IEEE INFOCOM*, Barcelona, Spain, 2006.

[22] Q. Li, D.-M. Chiu, and J. Lui, "On the practical and security issues of batch content distribution via network coding," in *Proc. 14th IEEE ICNP*, Washington, DC, USA, 2006.

[23] D. Kamal, D. Charles, K. Jain, and K. Lauter, "Signatures for network coding," in *Proc. 40th Annu. Conf. Inform. Sci. Syst.*, Princeton, NJ, USA, 2006.

[24] Z. Yu, Y. Wei, B. Ramkumar, and Y. Guan, "An efficient signature- based scheme for securing network coding against pollution attacks," in *Proc. IEEE INFOCOM*, Phoenix, AZ, USA, 2008.

ISSN: 2278 – 1323

[25] E. Kehdi and B. Li, "Null keys: Limiting malicious attacks via null space properties of network coding," in *Proc. IEEE INFOCOM*, Rio de Janeiro, Brazil, 2009.
[26] Z. Yu, Y. Wei, B. Ramkumar, and Y. Guan, "An efficient scheme for securing xor network coding against pollution attacks," in *Proc. IEEE INFOCOM*, Rio de Janeiro, Brazil, 2009.
[27] T. Ho *et al.,* "Byzantine modification detection in multicast net- works with random network coding," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2798–2803, Jun. 2008.
[28] S. Jaggi *et al.,* "Resilient network coding in the presence of byzantine adversaries," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2596–2603, Jun. 2008.
[29] R. Koetter and F. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3579–3591, Aug. 2008.
[30] Y. Li and J. C. Lui, "Stochastic analysis of a randomized detection algorithm for pollution attack in P2P live streaming systems," *Perform. Evaluation*, vol. 67, no. 11, pp. 1273–1288, 2010.
[31] Y. Li and J. Lui, "Identifying pollution attackers in network- coding enabled wireless mesh networks," in *Proc. 20th ICCCN*, Maui, HI, USA, Aug. 2011, pp. 1 –6.
[32] Y. Li and J. Lui, "Epidemic attacks in network-coding enabled wireless mesh networks: Detection, identification and evalua- tion," *IEEE Trans. Mobile Comput.*, vol. 12, no. 11, pp. 2219–2232, Nov. 2013.
[33] X. Jin and S.-H. G. Chan, "Detecting malicious nodes in peer-to-peer streaming by peer-based monitoring," *ACM Trans. Multimedia Comput. Commun. Appl.*, vol. 6, no. 2, pp. 9:1–9:18, Mar.2010

R.Ananthi ,Currently she is pursuing M.E (CSE) at Krishnasamy College of Engineering & Technology, Cuddalore, Tamil Nadu, India. Her research areas are Cloud Computing, Data Mining, MANET, wireless network and Big Data. She had attended many workshops also interested in attending seminars and conferences in various technologies.

J. Jayapradha received the M.E degree in Computer Science and Engineering from Anna University, Chennai in 2008. She is currently working as Assistant Professor in Krishnasamy College of Engineering and Technology. She has published few papers in National and International conferences and journals. Her area of interests includes Operating system, Compiler design, Software engineering. She is a member of ISTE.

ISSN: 2278 – 1323