PROVEST: AN EFFICIENT PROVENANCE TRUST MODEL FOR DELAY TOLERANT NETWORKS

TADI DURGA PRASANTH [#1], D.KANAKA DURGA[#2], K.RAMBABU[#3]

[#1] MCA Student, Master of Computer Applications,
D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

[#2] Assistant Professor, Master of Computer Applications,
D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

[#3] Head & Assistant Professor, Master of Computer Applications,
D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India

ABSTRACT

Delay tolerant networks (DTNs) are typically encountered in military network environments wherever end to-end property isn't secure because of frequent disconnection or delay. This work prefer a provenance-based trust model, specifically PROVEST (PROVENANCE primarily based Trust model) that aims to attain correct end to end trust assessment and maximize the delivery of correct messages received by destination nodes whereas minimizing message delay and communication overhead. Here we try to create some attacks inside the network and observe whether provenance can able to send the data under a new path or not. Here the term provenance acts like a buffer which can guarantee the packets to the destination node without any loss inside the communication. We conduct a comparative performance analysis of PROVEST by using socket programming and swings, networking package to observe the performance of current protocol.

Key Words:

Provest, Socket, Destination, Delivery

I. INTRODUCTION

Deferral or interruption open minded systems (DTNs) are frequently seen in developing applications, for example, crisis reaction, unique tasks, shrewd conditions, natural surroundings checking, and vehicular impromptu systems where different hubs participatein bunch

interchanges to accomplish a typical crucial. The center trait of DTNs is that there is no assurance of start to finish availability, in this manner causing high postponement or interruption because of inalienable qualities or deliberately acting mischievously hubs.

A significant test of a provenance-based framework is that it must guard against aggressors who may alter or drop messages including provenance data or spread phony data. Postponement lenient systems administration (DTN) is a way to deal with PC organize design that tries to address the specialized issues in heterogeneous systems that may need nonstop system availability. Instances of such systems are those working in portable or extraordinary earthbound conditions, or arranged systems in space. As of late, the term interruption lenient systems administration has picked up cash in the United States because of help from DARPA, which has subsidized numerous DTN ventures. Interruption may happen as a result of the restrictions of remote radio range, scantily of versatile hubs, vitality assets, assault, and clamor.

The capacity to ship, or course, information from a source to a goal major capacity all correspondence systems must have. Postponement and interruption open minded systems (DTNs), are described by their absence of network, bringing about an absence of immediate start to finish ways. In these difficult conditions, well known adhoc steering conventions, for example, AODV and DSR neglect to build up courses. This is because of these conventions attempting to initially build up a total course and afterward, after the course has been set up, forward the real data.However, when immediate start to finish ways are troublesome or difficult to set up, steering conventions must take to a "store and forward" approach, where information is gradually moved and put away all through the system with the expectation that it will in the long run arrive at its goal. A typical procedure used to augment the likelihood of a message being effectively moved is to repeat numerous duplicates of the message with the expectation that one will prevail with regards to arriving at its goal. This is practical just on systems with a lot of nearby stockpiling and bury hub data transfer capacity comparative with the normal traffic.

II. LITERATURE SURVEY

In this section we will mainly discuss about the background work that is carried out in order to prove the performance of our proposed Method. Now let us discuss about them in detail

MOTIVATION

1) Detecting and Localizing Wireless Spoofing Attacks

Remote systems are defenseless against mocking assaults, which takes into consideration numerous different types of assaults on the systems. Despite the fact that the character of a hub can be confirmed through cryptographic verification, validation isn't generally conceivable on the grounds that it requires key administration and extra infrastructural overhead. In this paper we propose a technique for both recognizing mocking assaults, just as finding the places of enemies playing out the assaults. We initially propose an assault finder for remote ridiculing that uses K-implies bunch investigation. Next, we depict how we coordinated our assault indicator into a continuous indoor restriction framework, which is likewise equipped for confining the places of the aggressors. We at that point show that the places of the assailants can be confined utilizing either territory based or point-based limitation calculations with indistinguishable relative mistakes from in the typical case. We have assessed our techniques through experimentation utilizing both a 802.11 (WiFi) organize just as a 802.15.4 (ZigBee) arrange. Our outcomes show that it is conceivable to identify remote mocking with both a high location rate and a low bogus positive rate, along these lines giving solid proof of the viability of the K-implies satirizing identifier just as the assault localizer.

2) Access directs weaknesses toward DoS assaults in 802.11 systems

We depict conceivable forswearing of administration assaults to framework remote 802.11 systems. To complete such assaults just item equipment and programming parts are required. The outcomes show that genuine weaknesses exist in various passageways and that a solitary vindictive station can without much of a stretch thwart any authentic correspondence inside a fundamental assistance set.

3) Detecting Identity Based Attacks in Wireless Networks Using Signal prints

Remote systems are powerless against numerous personality based assaults in which a malignant gadget utilizes fashioned MAC delivers to take on the appearance of a particular customer or to make different ill-conceived characters. For instance, a few connection layer benefits in IEEE 802.11 systems have been demonstrated to be defenseless against such assaults in any event, when 802.11i/1X and other security instruments are conveyed. In this paper we show that a sending gadget can be vigorously recognized by its sign print, a tuple of sign quality qualities detailed by passageways going about as sensors. We show that, not the same as MAC addresses or other parcel substance, assailants don't have as much control in regards to the signalprints they produce .Moreover, utilizing estimations in a testbed arrange, we exhibit that signalprints are unequivocally corresponded with the physical area of customers, with comparable qualities discovered generally in closeness. By labeling dubious bundles with their comparing signalprints, the system can vigorously recognize every transmitter freely of parcel substance, permitting location of a huge class of character based assaults with high likelihood.

4) Secure and Efficient Key Management in Mobile Ad Hoc Networks

In portable impromptu systems, because of temperamental remote media, have portability and absence of framework, giving secure correspondences is a major test in this interesting system condition. Normally cryptography procedures are utilized for secure correspondences in wired and remote systems. The hilter kilter cryptography is broadly utilized on account of its flexibility (validation, uprightness, and privacy) and straightforwardness for key conveyance. In any case, this methodology depends on a brought together system of open key foundation (PKI). The symmetric methodology has calculation proficiency, yet it experiences possible assaults on key understanding or key appropriation. Truth be told, any cryptographic methods is incapable if the key administration is feeble. Key administration is a focal viewpoint for security in portable impromptu systems. In versatile specially appointed systems, the computational burden and intricacy for key administration is emphatically dependent upon limitation of the hub's accessible assets and the dynamic idea of system geography.

III. EXISTING METHODOLOGY

In a multi-hop wireless network, all the nodes cooperate in relaying/routing traffic. In the existing system there is no concept like detect and prevent for the packet dropping and packet modifiers. In the existing system there is no concept like counter measure for the attacks which occur during the data transfer.

LIMITATIONS OF THE EXISTING METHODOLOGY

The following are the limitation of existing system. They are as follows:

1. There is no method to provide counter measure for that packets dropping or packet modifiers attack.
2. Data security is very less due to insider attacks
3. All the existing approaches failed in identifying the attacks during data transmission and provide an alternate path for the data transfer.
4. All the existing approaches try to use static path identifiers and they used to send all the packets in that static predefined paths.
5. In the existing networks the adversary try to behave as a genuine user or genuine node and try to inject the information illegally .
6. In the existing networks the adversary try to drop the packets illegally by making the node absence or by creating a link failures.
7. In the existing networks there was no method which can provide counter measure for the attackers dynamically. All the attacks that occur will be identified at the later time.

IV. PROPOSED METHODOLOGY

In this project, we develop an accurate algorithm like provest for detecting selective packet drops made by insider attackers. Our algorithm also provides a truthful and publicly verifiable decision statistics as a proof to support the detection decision. In our proposed method we try to identify the malicious users who try to create packets dropping or packet modifying during data communication and try to provide a counter measure for the attacked node. The provest will try to provide an alternate path for the failure node and send the packets to valid destination under a dedicated path.

ADVANTAGES OF THE PROPOSED SYSTEM

The following are the advantages of the proposed system. They are as follows:

1. The proposed system with new provest construction is best in sending the packets under a dedicated path.
2. The proposed system gives the advantage of privacy-preserving.
3. Our construction incurs low communication and storage overheads at intermediate nodes.
4. The proposed method is best in providing security for the data at the time of packet dropping or packet modifiers.

IV. IMPLEMENTATION STAGE

Implementation Stage is where the hypothetical structure is changed over into automatically way. In this stage we will partition the application into various modules and afterward coded for arrangement. The application is separated essentially into following 4 modules. They are as follows:

1. Topology creation
2. Network construction
3. Analysis of normal Case and Attack Case
4. Data Transmission

Now let us discuss about each and every module and sub modules which are present in this application.

1) Topology Creation Module

In this module ,initially for performing any type of data communication task over a set of nodes, we need to create a topology with a set of nodes like source or sender ‘s’ and a router window and a set of destination nodes like Node A,Node B...Node E.Here as wireless sensor networks have no fixed topology in real time, but in our proposed application we create a

mesh topology in which the data which should be transferred from source to destination chooses a best path for sending that to the valid receivers.

2) **Network Construction Module**

In this module initially after creating the topology with a set of nodes having router as a main node within the network. This network construction module plays a very important role where the data which is send to be send from a valid source node should be browse at the sender window and he need to choose a valid destination node with a set of intermediate nodes like Node A,...Node E.Now the data which is browsed by the sender node will not be directly passed from sender to destination but this will be initially passed to the router window. Where the router will identify the individual node status and apply PROVEST with auto correlation technique to check which node has any link or node failure.If a node with such a change in its topology is observed by the router window during data transfer then the router will immediately guide a new route for the destination from that attack point.

3) **Analysis of Normal Case and Attack Case Module**

In this module the data which is to be transferred is identified and observed in two different cases like :One in normal case and other is in Attack or Failure case.Initailly if we don't create any attack either from internal or external nodes and user try to send data from a valid sender node to destination node.Then such a data transfer is treated as a normal mode transfer.If the same data is transferred through any intermediate node failure either through low energy level or link failure ,then such a data transfer is treated as a attack case and this will be clearly identified by the router which is monitoring whole network

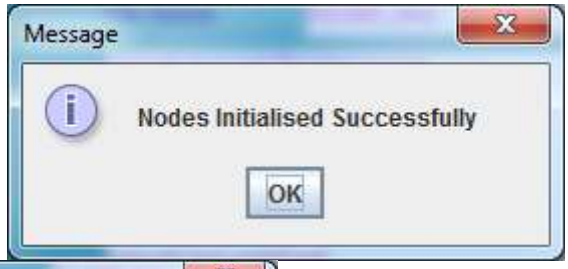
4) **Data Transmission Module**

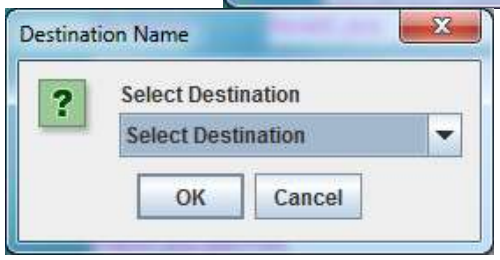
In this module all the sender node tries to pass the information from a valid intermediate path to the valid destination node with no attack or no packet loss. If such a communication is done the data is reached successfully at the receiver side and such a situation is known as normal case. If the same data is travelling through a failure node or failure path, then we need to apply PROVEST algorithm with auto correlation technique so that PROVEST will send the data in an alternate path from the point where the node is attacked.The main motto of this module is data

should be transferred from a valid source node to destination node with no packet loss in any manner.

V. EXPERIMENTAL REPORTS

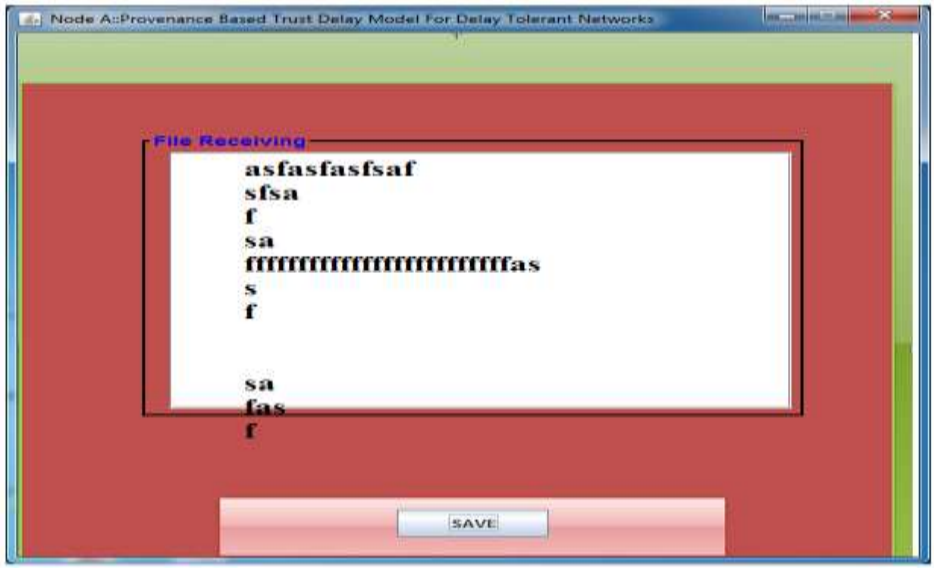
SENDER WILL CHOOSE SOME PROPERTIES FOR SENDING THE DATA





PROVEST ROUTER IS STARTED FOR RECEIVING THE DATA

DESTINATION WINDOW WILL RECEIVE THE DATA



VI. CONCLUSION

In this paper, we showed that compared with conventional detection algorithms that utilize only the distribution of the number of lost packets, exploiting the correlation between lost packets significantly improves the accuracy in detecting malicious packet drops. Such improvement is especially visible when the number of maliciously dropped packets is

comparable with those caused by link errors. To correctly calculate the correlation between lost packets, it is critical to acquire truthful packet-loss information at individual nodes.

VII. REFERENCES

[1] H. Lim, Y. Moon, and E. Bertino, "Provenance-based trustworthiness assessment in sensor networks," in *Proc. of Data Management for Sensor Networks*, 2010, pp. 2–7.

[2] I. Foster, J. Vockler, M. Wilde, and Y. Zhao, "Chimera: A virtual data system for representing, querying, and automating data derivation," in *Proc. of the Conf. on Scientific and Statistical Database Management*, 2002, pp. 37–46.

[3] K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer, "Provenance-aware storage systems," in *Proc. of the USENIX AnnualTechnical Conf.*, 2006, pp. 4–4.

[4] Y. Simmhan, B. Plale, and D. Gannon, "A survey of data provenance in e-science," *SIGMOD Record*, vol. 34, pp. 31–36, 2005.

[5] R. Hasan, R. Sion, and M. Winslett, "The case of the fake picasso: Preventing history forgery with secure provenance," in *Proc. Of FAST*, 2009, pp. 1–14.

[6] S. Madden, J. Franklin, J. Hellerstin, and W. Hong, "TAG: a tiny aggregation service for ad-hoc sensor networks," *SIGOPS Operating Systems Review*, no. SI, Dec. 2002.

[7] K. Dasgupta, K. Kalpakis, and P. Namjoshi, "An efficient clustering based heuristic for data gathering and aggregation in sensor networks," in *Proc. of Wireless Communications and Networking Conference*, 2003, pp. 1948–1953.

[8] S. Sultana, E. Bertino, and M. Shehab, "A provenance based mechanism to identify malicious packet dropping adversaries in sensor networks," in *Proc. of ICDCS Workshops*, 2011, pp. 332–338.

[9] L. Fan, P. Cao, J. Almeida, and A. Z. Broder, "Summary cache: a scalable wide-area web cache sharing protocol," *IEEE/ACM Trans. Netw.*, vol. 8, no. 3, pp. 281–293, Jun. 2000.

[10] A. Kirsch and M. Mitzenmacher, "Distnce-sensitive bloom filters," in *Proc. of the Workshop on Algorithm Engineering and Experiments*, 2006, pp. 41–50.

[11] C. Rothenberg, C. Macapuna, M. Magalhaes, F. V rdi, and A. Wiesmaier, "In-packet bloom filters: Design and networking applications," *Computer Networks*, vol. 55, no. 6, pp. 1364 – 1378, 2011.

[12] M. Garofalakis, J. Hellerstein, and P. Maniatis, "Proof sketches: Verifiable in-netwok aggregation," in *ICDE*, 2007, pp. 84–89.

[13] T. Wolf, "Data path credentials for high-performance capabilitiesbased networks." in *Proc. of ACM/IEEE Symp. on Architectures for Networking and Communications Systems.*, 2008, pp. 129–130.

[14] H. Chan, A. Perrig, and D. Song, "Secure hierarchical in-network aggregation in sensor networks," in *Proc. of the conf. on Computer and communications security (CCS)*, 2006, pp. 278–287.

[15] S. Roy, M. Conti, S. Setia, and S. Jajodia, "Secure data aggregation in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 1040–1052, 2012.