ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

EBoX: Evidence of Behaviour Information Exchange Mechanism against Selfish Attacks

Santhosh J [1], Malini V K [2]

Assistant Professor, Dept. of Computer Science, Sree Narayana Guru College, Coimbatore, Tamil Nadu, India[1]

M.Phil Scholar, Dept. of Computer Science, Sree Narayana Guru College, Coimbatore, Tamil Nadu, India[2]

ABSTRACT: Mobile ad-hoc networks (MANETs) are forced to cooperate in order to work properly. This cooperation is a cost effective activity and some nodes can refuse to cooperate with other nodes that leading to selfish node behavior. This is how the overall network performance will be seriously affected. The use of watchdogs is a well known mechanism to detect selfish nodes but this watchdog process fails due to generating false positives and false negatives that can induce to wrong operations and also relying on local watchdogs alone can lead to poor performance when detecting selfish nodes, in term of precision and speed. This is especially important on networks with periodic contacts, such as delay tolerant networks (DTNs), where sometimes watchdog's lack of enough time or information to detect the selfish nodes. This study proposes an Evidence of Behavior Information Exchange (EBoX) scheme as a collaborative approach based on the diffusion of local selfish nodes awareness when a node is compromised by external attackers. The EBoX approach reduces the packet transmission time and increases the precision by detecting the compromised nodes attacked by selfish nodes. The EBoX helps to avoid partial selfish nodes using anonymization technique, this technique hides the nodes original identity and provides an anonymous access, this helps to avoid partial selfish nodes in the network. Reputation values will be calculated according to their contact log and transmission logs.

KEYWORDS: Behavior, Trust, Information exchange, Reputation, Selfish attack Recommender system

I. INTRODUCTION

Cooperative networks are gaining an increasing interest in information and communications technologies since such networks can improve communication capability and provide a fertile environment for the development of context-aware services. Cooperative communications and networking represent a new paradigm which involves both transmission and distributed processing, promising significant increase of capacity and diversity gain in wireless networks. From one hand, the integration of long-range and short-range wireless communication networks (e.g., infra structured networks such as 3G, wireless ad hoc networks, and wireless sensor networks) improves the performance in terms of both area coverage and quality of service (QoS). On the other hand, the cooperation among nodes, as in the case of wireless sensor networks, allows a distributed space-time signal processing which enables, among others, environmental monitoring, localization techniques, and distributed measurements, with a reduced complexity or energy consumption per node. The relevance of this topic is also reflected by numerous technical sessions in current international conferences as well as by the increasing number of national and international projects on these aspects.

SELFISH NODE BEHAVIOUR:

Several nodes will be participated in the MANET for data forwarding and data packets transmission between source and destination. All the nodes of MANET will perform the routing function as mandatory. They must forward the traffic which other nodes sent to it. Among all the nodes some nodes will behave selfishly, these nodes are called selfish nodes. MANET is a Dynamic Topologies Bandwidth constrained, variable capacity links Power constrained operations limited physical security.

A. Dynamic topologies: Nodes are free to move arbitrarily; thus the topology of the network may change randomly and rapidly at unpredictable times in network. Modification of transmission and reception parameters such as power may also impact the topology.

B. Bandwidth constrained: variable capacity links Wireless links will continue to have significantly lower capacity than their hard-wired counter parts. The relatively low to moderate link capacities will leads to the congestion rather than the exception.

C. Power-constrained operations: Some or all the nodes in a MANET rely on batteries for their energy. Thus, for these nodes, the most vital design problem may be that of power conservation. Any node in MANET may act selfishly, which means, using its limited resource only for its own profit, since each node in a network has resource constraints, such as storage and battery limitations.

A node would like to enjoy the profits provided by the resources of other nodes in the network, but however it should not make its own resource accessible to help others. Existing exploration on selfish behaviors in a MANET mainly focus on network concerns. For network problems at MANET may be as some selfish nodes may not transmit data to others to conserve their own battery constraints. Even though network disputes at MANET are important, replica allocation is also critical, ever since the vital goal of using a MANET is to provide data services to users. The problem because of replica allocation refers as if a selfish node may not share its own memory space to store replica for the benefit of other nodes. Selfish replica allocation refers to a node's non cooperative action, such that the node refuses to cooperate fully in sharing its memory space with other nodes.

TYPES OF SELFISH ATTACKS:

Selfish attacks are different depending on what and how they attack in order to pre-occupy CR spectrum resources. There are three different selfish attack types

Attack Type 1

A Type 1 attack is designed to prohibit a legitimate SU (LSU) from sensing available spectrum bands by sending faked PU signals. The selfish SU (SSU) will emulate the characteristics of PU signals. A legitimate SU who overhears the faked signals makes a decision that the PU is now active and so the legitimate SU will give up sensing available channels. This attack is usually performed when building an exclusive transmission between one selfish SU and another selfish SU regardless of the number of channels. There must be at least two selfish nodes for this type of attack.

Attack Type 2

Type 2 attacks are also a selfish SU emulating the characteristics of signals of a PU, but they are carried out in dynamic multiple channel access. In a normal dynamic signal access process, the SUs will periodically sense the current operating band to know if the PU is active or not, and if it is, the SUs will immediately switch to use other available channels. In this attack type, a continuous fake signal attack on multiple bands in a round-robin fashion, an attacker can effectively limit legitimate SUs from identifying and using available spectrum channels.

Attack Type 3

In Type 3, called a channel pre-occupation selfish attack, attacks can occur in the communication environment that is used to broadcast the current available channel information to neighboring nodes for transmission. We consider a communication environment that broadcasting is carried out through a common control channel (CCC) which is a channel dedicated only to exchanging management information. A selfish node will broadcast fake free (or available) channel lists to its neighboring SUs Even though a selfish SU only uses three channels, it will send a list of all five occupied channels. Thus, a legitimate SU is prohibited from using the two available channels. Detection of existing selfish technologies is likely to be uncertain and less reliable, because they are based on estimated reputation or estimated characteristics of stochastic signals.

II. RELATED WORK

Abbas, Sonya Proposed [1] an RSS-based detection mechanism in to safeguard the network against Sybil attacks. The scheme worked on the MAC layer using the 802.11 protocol without the need for any extra hardware demonstrated through various experiments that a detection threshold exists for the distinction of legitimate new nodes and new malicious identities confirmed this distinction rationale through simulations and through the use of a real-world test bed of Sun SPOT sensors. This study also showed the various factors affecting the detection accuracy, such as network connections, packet transmission rates, node density, and node speed. The main disadvantage Need additional hardware to demonstrate and failed to tackle Masquarding attacks.

[2] The objective of OCEAN is to avoid this trust-management machinery and direct first-hand observations of other nodes' behavior. OCEAN schemes requiring second-hand reputation exchanges. In [3] Bansal, Sorav, and Mary Baker shows reputation systems for self policing and adaptation to network cooperation can be built, and how they can mitigate the deleterious effects of misbehavior in self-organized networks by using monitoring to generate reputation ratings which in turn allow nodes to make informed decisions about their response to the behavior of other nodes and have described how second-hand information can be used to improve the response, while avoiding the dangers of rumor spreading.

[5] Is proposed one of the fundamental reasons for the discrepancy on the tail behavior of intermeeting time between the recent empirical data and the theoretical/simulation results based on most of the current mobility models is the finite boundary with respect to the timescale of interest. These guidelines on scaling the size of the domain also help better understand the true role of the boundary .It provides guidelines on mobility modeling, performance analysis, and protocol design but not integrated with attack detection techniques. [6] Brings new practical recommendations to evaluate the performance of forwarding algorithms. Most of the mobility models characterized by a light tailed inter contact time distribution for any pair of nodes.

[8] COMMIT protocol for individually rational, truthful, and energy-efficient routing in ad hoc networks. To the best of our knowledge, this is the first ad hoc routing protocol with these features. COMMIT is based on the VCG payment scheme in conjunction with a novel game-theoretic technique to achieve truthfulness for the sender node.

Hernandez-Orallo, given a new collaborative watchdog approach in [10] modeled its performance using a Continuous Time Markov Chain with two parameters to indicate the degree of collaboration and detection of the watchdog. This reduction is very significant when the watchdog detection effectiveness is low.

III. PROPOSED SYSTEM

The proposed EBoX (*Evidence of Behavior Information Exchange*) technique used to detect node misbehaviors such as selfish attacks in the network based on the node trust performance behavior. In this technique server protocol continuously monitor the network nodes collectively detect and declare the misbehavior of a suspicious node. This EBoX performs under all routing table declaration then propagated throughout the network so that the misbehaving node will be cut off from the rest of the network. And the selfish nodes will be punished and good nodes will be prioritized along with credit point.

The proposed system overcomes the above drawback of watchdog by implementing a new method which is the combination of Reputation based schemes. Data anonymization techniques help to prevent from partial selfishness attackers. Based on the reputation score and positive score selfish node will be identified and punished according to their reputation score, and the best node will be elected as a CH.

Anonymous Key generation and authentication: The Anonymous Key generation performed in this EBoX mechanism and it initially applies the random key generation algorithm/RSA algorithm can be used for Anonymous Key generation. Additionally the key verification and authentication is required to ensure that services are offered to legitimate entities.

Decision making: The process of estimating the node trust by proving the collected evidences are true or false by judging the routing behaviors and the mobile nodes are categorized as trusted/selfish and genuine/ malicious.

Trust estimation: The monitor compares the collected evidence data with the predefined threshold value and finds the deviation. Based on the information collected and compared by the user, it calculates the direct trust value and stores it into the local table RT (reputation table). The direct trust value is calculated mainly based on the behavior of packet

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

forwarding, dropping and tampering. This reputation trust value is determined based on the information collected from other users in the network and maintained by the common RT.

Reputation or Trust Analysis: Any node present in the network suspects the malicious activity such as holding the packets for a long time or providing false report as an acknowledgement by any node in the network then it can send evidence at once to the network monitor. The time receiving evidence from any node in the network by server then the server proves the evidence by following the information exchange process if the node is proved as a good performer node then the genuine user has to send a maximum of one cooperation message using the tag base published in the setup procedure. If the node does not send cooperation (one time) or sends multiple cautions is marked as a malicious node.

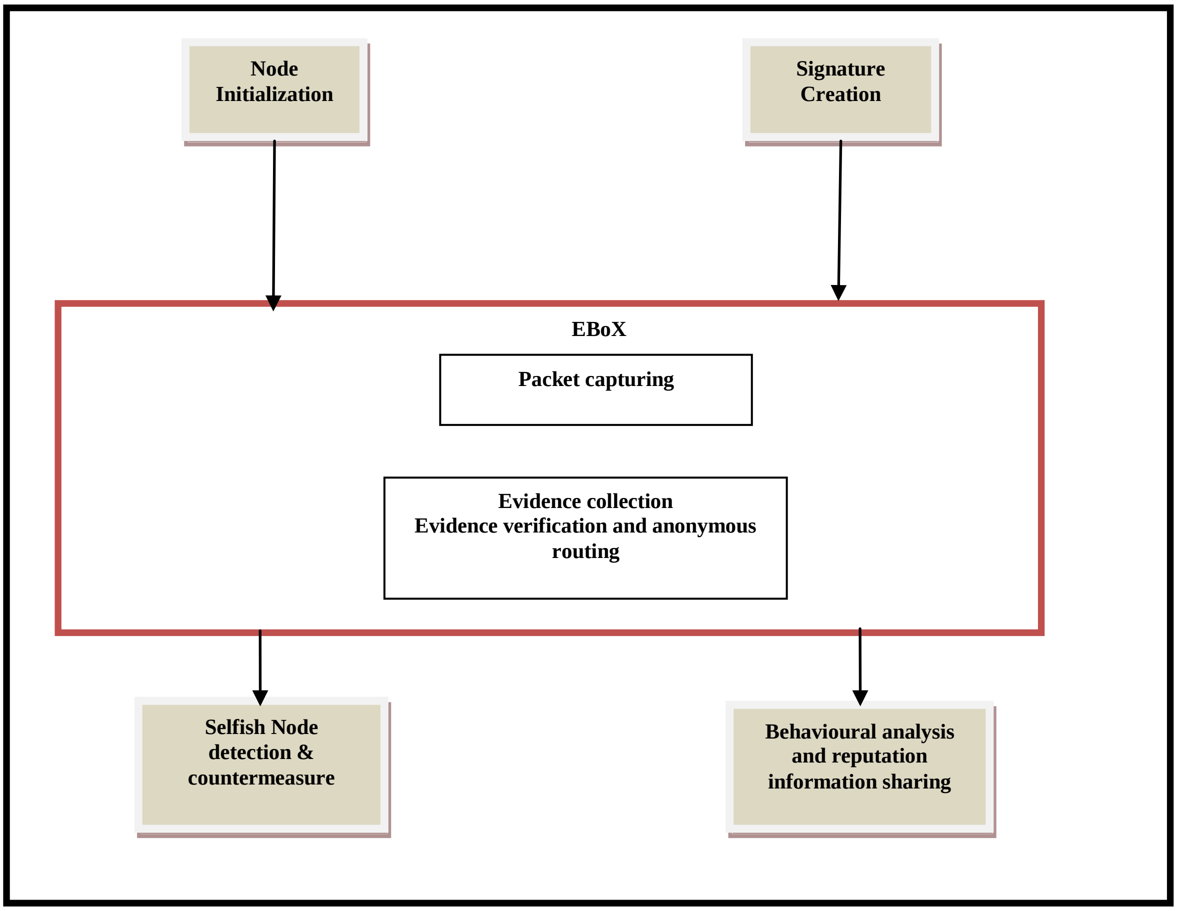
Node Initialization
Signature Creation
EBoX
Packet capturing
Evidence collection
Evidence verification and anonymous routing
Selfish Node detection & countermeasure
Behavioural analysis and reputation information sharing

Fig 1: Architecture Diagram of EBoX

Anonymous routing in EBoX:
This section describes the anonymous routing scheme for fast and secure transmission to obtain privacy and Concealed data transmission of the data in the network against selfishness attack
Input: Mn (Number of Mobile nodes), a-id (anonymous id)
Output: Secure and privacy preserved data transmission.
Steps:
1. Activate the EBoX _CH
2. Register and active a mobile node Mn1….Mnn and provide a private key (Pk). And also provide a public ID.
3. Secret Key generated SK= KG(Pk,ID) where KG key generator Pk access policy ID identity of the particular user.
4. Source generates Anonymous Route AR= data transmit (Msk, PubK) where MSK is master secret key, PubK

DOI: 10.15680/IJIRCCE.2015. 0309087

```
    Public Key
 5. for each node, (RIX-sample message)
 Send RIX m (sender, receiver, seqno, Pk)
 6. If (Node seq no == largest seq no)
 Select node as best hop and Update routing table.
 7. Sender transmits RIX,id (M) to its best hop.
 8. Best hop forwards RIX_ack,id(M) to its best hop.
 9. Receiver RIX r,id(M) to get the original message.
 10. Provides route anonymity, sender anonymity, and receiver anonymity using Pk, pubk and rid.
 11. Monitor the node behavior and elect CH
 12. Report and update the routing table.
```

During the initial setup phase, the EBoX generates a group key (public/private key pair) and sends announcement with group public key during gateway advertisement. In addition, EBoX also publishes the method of generating the tag bases that will be used to send caution, cooperation and event reporting.

IV. EXPERIMENT AND ANALYSIS

The EBoX mechanism is working perfectly on the network communication. It works on the highly scalable environment too. The attacker detection is performed by each node by verifying the key on the header packet. If the data integrity is changed then the polluter node will be identified by comparing the key with the previous key. This is how the system is detecting the polluter node in the network. The following chart is described the accuracy level of detecting the pollution nodes whenever the scalability increased. This is a comparison chart of existing and proposed accuracy levels.

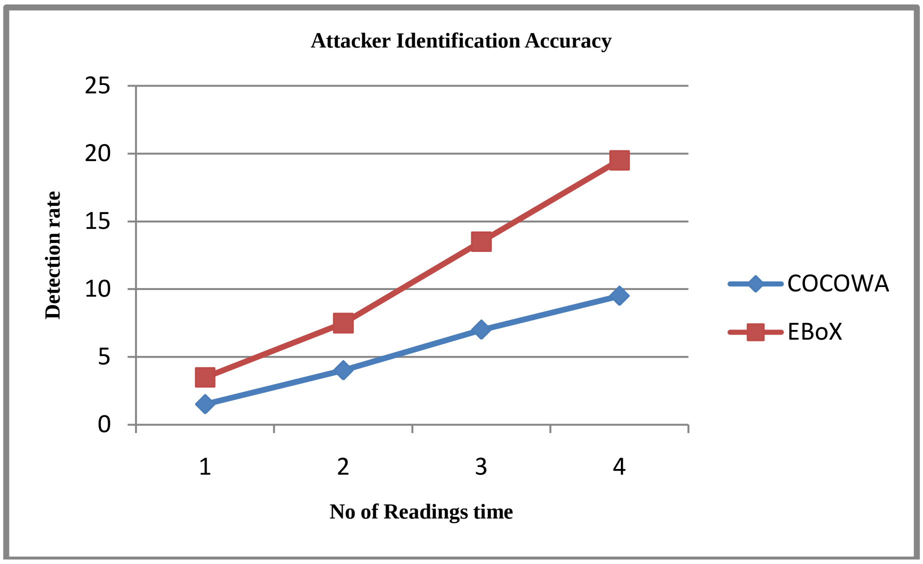

Fig 2: Attacker Identification chart

Delay Analysis:

Delay is the important factor to be considered in all type of network communication. The system should give reliability, integrity, scalability with no time delay. The following table contains the experimented time taken for the data transmission (in seconds) for existing and proposed. With the experimented values the graph is generated to represent the proposed system performance.

DOI: 10.15680/IJIRCCE.2015. 0309087

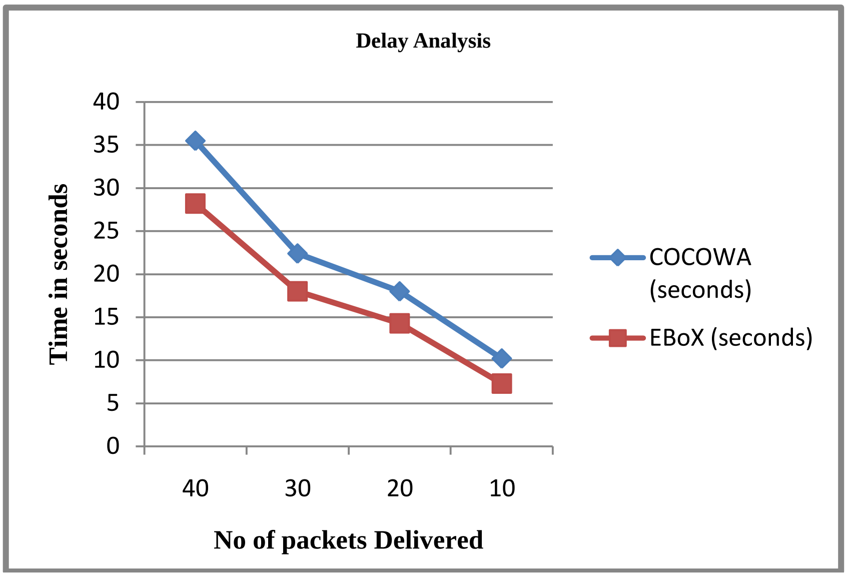

Fig 3: Delay Analysis chart

V. CONCLUSION

The EBoX addresses the privacy and selfishness attack issues in MANET. The architecture adapts the mechanisms such as EBoX, trust estimation, reputation exchange in order to monitor and determine the mobile nodes trust and reputation. Based on these behavioral factors report server decides the node state and reports to the other users in the network. It also provides anonymous data transformation in order to prevent data from partial selfishness nodes. If the nodes are continuously attack the network by doing selfish behavior then the nodes will get penalty by the server or monitor and the better performer nodes will get reward points from the network server or monitor.

REFERENCES

[1]Abbas, Sonya, et al. "Lightweight Sybil attack detection in MANETs." *Systems Journal, IEEE* 7.2 (2013): 236-248.
[2]Bansal, Sorav, and Mary Baker. "Observation-based cooperation enforcement in ad hoc networks." *arXiv preprint cs/0307012* (2003).
[3] Buchegger, Sonja, and J-Y. Le Boudec. "Self-policing mobile ad hoc networks by reputation systems." Communications Magazine, IEEE 43.7 (2005): 101-107.
[4]Buttyán, Levente, and Jean-Pierre Hubaux. "Enforcing service availability in mobile ad-hoc WANs." *Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing*. IEEE Press, 2000.
[5] Cai, Han, and Do Young Eun. "Crossing over the bounded domain: from exponential to power-law inter-meeting time in manet." *Proceedings of the 13th annual ACM international conference on Mobile computing and networking*. ACM, 2007.
[6] Chaintreau, Augustin, et al. "Impact of human mobility on opportunistic forwarding algorithms." *Mobile Computing, IEEE Transactions on* 6.6 (2007): 606-620.
[7] Chaintreau, Augustin, et al. "Impact of human mobility on opportunistic forwarding algorithms." *Mobile Computing, IEEE Transactions on* 6.6 (2007): 606-620.
[8] *Eidenbenz, Stephan, Giovanni Resta, and Paolo Santi. "The COMMIT protocol for truthful and cost-efficient routing in ad hoc networks with selfish nodes."Mobile Computing, IEEE Transactions on 7.1 (2008): 19-33.*
[9]*Gao, Wei, et al. "Multicasting in delay tolerant networks: a social network perspective." Proceedings of the tenth ACM international symposium on Mobile ad hoc networking and computing. ACM, 2009.*
[10] *Hernandez-Orallo, Enrique, et al. "Improving selfish node detection in MANETs using a collaborative watchdog." Communications Letters, IEEE 16.5 (2012): 642-645.*

DOI: 10.15680/IJIRCCE.2015. 0309087