International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 12 Issue 2 –JANUARY 2015.

Enhanced MANET Data Security against BOTNET attacks using Hybrid IDS Model

*1Hemalatha.U, *2Mohana.P, *3Manjubargavi.A, *4SanjanaViswanathan and #5I.Varalakshmi Murugan

*UG Scholars (CSE) Manakula Vinayagar Institute of Technology, Puducherry, India

#Assistant Professor Manakula Vinayagar Institute of Technology, Puducherry, India

***Abstract*— In this paper, we propose a clustering method that uses hybrid CS for Mobile Ad-hoc Networks. The Mobile nodes are organized into clusters. Within a cluster, nodes transmit data to cluster head (CH) without using CS. CHs use CS to transmit data to sink. We first propose an analytical model that studies the relationship between the size of clusters and number of transmissions in the hybrid CS method, aiming at finding the optimal size of clusters that can lead to minimum number of transmissions. Then, we propose a k-means Clustering algorithm based on the results obtained from the analytical model. Finally, we present a distributed implementation of the clustering method. Extensive simulations confirm that our method can reduce the number of transmissions significantly. We then improve the system by adding security features in data transmission. And also detect false node (using watchdog mechanism) should alert the source and remove the node. In addition also detect BOTNET (using both anomaly and signature based IDS) and alert the source and remove the node. At last we show the performance analysis with various parameters are resulting the improvement of our system**

Index Terms—Access control, secure data transmission, privacy preserving, Cluster Head, MANET, BOTNET, clustering, K-means algorithm

I. Introduction

Nowadays A fundamental characteristic [1] of wireless ad hoc networks is the time difference of the channel potency of the original communication links. Such time difference occur at numerous occasion scales and can be owing to multipath desertion, pathway loss using space attenuation, shadowing by obstacles, and intrusion from extra users. The impact of such time difference on the design of wireless ad hoc networks permeates throughout the layers, ranging from coding and power control at the physical layer to cellular handoff and coverage planning at the networking layer. An important means to cope with the time variation of the channel is the use of diversity. The basic design is to recover presentation by creating numerous autonomous signal ways flanked by the source and the target nodes. These diversity modes pertain to a point-to-point link. Recent results point to another form of diversity, inherent in a wireless network with multiple users. Overall system throughput is maximized by allocating at any time the common channel resource to the user that can best exploit it. Similar results can be obtained for the downlink from the base station to the mobile users.

The wireless networks are classified into different types: Mobile ad-hoc networks, Mobile network, Delay Tolerance Networks, and so on. The term MANET (Mobile Ad hoc Network) refers to a multihop packet based wireless network composed of a set of mobile nodes that can communicate and move at the same time, without using any kind of fixed wired infrastructure. MANET is actually self organizing and adaptive networks that can be formed and deformed on-the-fly without the need of any centralized administration. Otherwise, a stand for “Mobile Ad Hoc Network” A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission.

There are many existing system are proposed previously to address security issues in Mobile Ad-hoc networks. In an existing system, Attribute Based Encryption ABE schemes are constructed on the architecture where a single trusted authority has the power to generate the whole private keys of users with its master secret information. The key escrow problem is inherent such that the key authority can decrypt every ciphertext addressed to users in the system by generating their secret keys at any time.

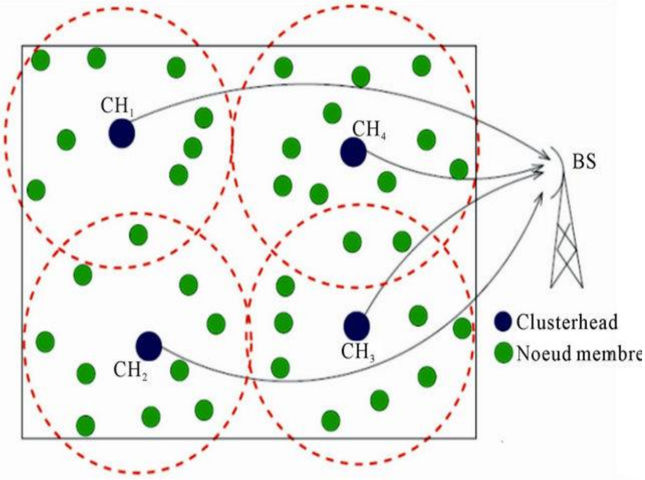

Figure 1 MANET Architecture with Cluster Head

The problem of applying the ABE to DTNs introduces several security and privacy challenges. Since some users may change their associated attributes at some point (for example, moving their region), or some private keys might be compromised, key revocation (or update) for each attribute is necessary in order to make systems secure. An Attribute Based Encryption is to improve upon the scalability of the above solutions; one-to-many encryption methods such as Attribute Based Encryption can be used. In order to overcome the following disadvantages in previous works: Key escrow problem in a multi-authority system, one-to-many encryption methods and Attribute revocation problems. First, immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability. Second, encryptors can define a fine-grained access policy using any monotone access structure under attributes issued from any chosen set of authorities. Third, the key escrow problem is resolved by an escrow-free key issuing protocol that exploits the characteristic of the decentralized DTN architecture. The key issuing protocol generates and issues user secret keys by performing a secure two-party computation (2PC) protocol among the key authorities with their own master secrets. The 2PC protocol deters the key authorities from obtaining any master secret information of each other such that none of them could generate the whole set of user keys alone. Thus, users are not required to fully trust the authorities in order to protect their data to be shared. The data confidentiality and privacy can be cryptographically enforced against any curious key authorities or data storage nodes in the proposed scheme in existing systems, No Clustering Methods, No Improved security features and there is no Intrusion Detection System. In order to overcome these tackles, the two metrics to evaluate the performance of the clustering with hybrid CS proposed in this paper: the number of transmissions which is required to collect data from mobiles to the sink and the reduction ratio of transmissions (reduction ratio for short) of our method compared with other methods.

Immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing vulnerability. In this paper, we attempt to enhance the existing secure date retrieval model of Mobile ad-hoc networks with some botnet attacks in communication. That is, unauthorized observers must be unable to detect the origin of such events by analyzing the network traffic and communication data. In this work, we present a new framework for modelling, analyzing, and evaluating anonymity with enhanced secure data transmission in Mobile ad-hoc networks by using high class Hybrid IDS Technique to address the BOTNET attacks.

The rest of the paper will be organised as follows: In section 2, we see about the related works of the paper. In section 3, we discuss about the proposed method. The implementation of our paper is in section 4. Our proposed system conclusion is in section 5.

II. RELATED WORK

As a promising communication paradigm, Cognitive Radio Networks (CRNs) have paved a road for Secondary Users (SUs) to opportunistically exploit unused licensed spectrum without causing unacceptable interference to Primary Users (PUs). In this paper, we study the distributed data collection problem for asynchronous CRNs, which has not been addressed before. First, we study the Proper Carrier-sensing Range (PCR) for SUs. By working with this PCR, an SU can successfully conduct data transmission without disturbing the activities of PUs and other SUs. Subsequently, based on the PCR, we propose an Asynchronous Distributed Data Collection (ADDC) algorithm with fairness consideration for CRNs. ADDC collects data of a snapshot to the base station in a distributed manner without any time synchronization requirement. The algorithm is scalable and more practical compared with centralized and synchronized algorithms. Through comprehensive theoretical analysis, we show that ADDC is order-optimal in terms of delay and capacity, as long as an SU has a positive probability to access the spectrum. Finally, extensive simulation results indicate that ADDC can effectively finish a data collection task and significantly reduce data collection delay.

The purpose of a wireless mobile network (WSN) is to provide the users with access to the information of interest from data gathered by spatially distributed mobiles. Generally the users require only certain aggregate functions of this distributed data. Computation of this aggregate data under the end-to-end information flow paradigm by communicating all the relevant data to a central collector node is a highly inefficient solution for this purpose. An alternative proposition is to perform in-network computation. This, however, raises questions such as: what is the optimal way to compute an aggregate function from a set of statistically correlated values stored in different nodes; what is the security of such aggregation as the results sent by a compromised or faulty node in the network can adversely affect the accuracy of the computed result. In this paper, we have presented an energy-efficient aggregation algorithm for WSNs that is secure and robust against malicious insider attack by any compromised or faulty node in the network. In contrast to the traditional snapshot aggregation approach in WSNs, a node in the proposed algorithm instead of unicasting its sensed information to its parent node, broadcasts its estimate to all its neighbors. This makes the system more fault-tolerant and increase the information availability in the network. The simulations conducted on the proposed algorithm have produced results that demonstrate its effectiveness.

Mobile networks are collection of mobile nodes which co-operatively send sensed data to base station. As mobile nodes are battery driven, an efficient utilization of power is essential in order to use networks for long duration hence it is needed to reduce data traffic inside mobile networks, reduce amount of data that need to send to base station. The main goal of data aggregation algorithms is to gather and aggregate data in an energy efficient manner so that network lifetime is enhanced. Wireless mobile networks (WSN) offer increasingly Mobile nodes need less power for processing as compared to transmitting data. It is preferable to do in network processing inside network and reduce packet size. One such approach is data aggregation which attractive method of data gathering in distributed system architectures and dynamic access via wireless connectivity. Wireless mobile networks have limited computational power and limited memory and battery power, this leads to increased complexity for application developers and often results in applications that are closely coupled with network protocols. In this paper, a data aggregation framework on wireless mobile networks is presented. The framework works as a middleware for aggregating data measured by a number of nodes within a network. The aim of the proposed work is to compare the performance of TAG in terms of energy efficiency in comparison with and without data aggregation in wireless mobile networks and to assess the suitability of the protocol in an environment where resources are limited.

Wireless Mobile Network is a field of research which is viable in every application area like security services, patient care, traffic regulations, habitat monitoring and so on. The resource limitation of small sized tiny nodes has always been an issue in wireless mobile networks. Various techniques for improving network lifetime have been proposed in the past. Now the attention has been shifted towards heterogeneous networks rather than having homogeneous mobile nodes in a network. The concept of partial mobility has also been suggested for network longevity. In all the major proposals; clustering and data aggregation in heterogeneous networks has played an integral role. This paper contributes towards a new concept of clustering and data filtering in wireless mobile networks. In this paper we have compared voronoi based ant systems with standard LEACH-C algorithm and MTWSW with TWSW algorithm. Both the techniques have been applied in heterogeneous wireless mobile networks. This approach is applicable both for critical as well as for non-critical applications in wireless mobile networks. Both the approaches presented in this paper outperform LEACH-C and TWSW in terms of energy efficiency and shows promising results for future work.

Wireless Mobile Networks have a wide range of applications including environmental monitoring. These networks consist of wireless mobile nodes which are densely deployed to provide a wider coverage area. The dense deployment of the mobile node provides spatial correlation in the network. In this paper an efficient data gathering approach is implemented by combining the dual prediction and clustering algorithm. Clustering algorithm based on spatial correlation is used to cluster the mobile nodes. Then within the cluster, the nodes send their data to the sink using the Normalized Least Mean Square dual prediction algorithm. Simulation results show that the proposed algorithm reduces the average energy consumption of the network.

In wireless mobile network [7], data fusion is considered an essential process for preserving mobile energy. Periodic data sampling leads to enormous collection of raw facts, the transmission of which would rapidly deplete the mobile power. In this paper, we have performed data aggregation on the basis of entropy of the mobiles. The entropy is computed from the proposed local and global probability models. The models provide assistance in extracting high precision data from the mobile nodes. We have also proposed an energy efficient method for clustering the nodes in the network. Initially, mobiles sensing the same category of data are placed within a distinct cluster. The remaining unclustered mobiles estimate their divergence with respect to the clustered neighbors and ultimately join the least-divergent cluster. The overall performance of our proposed methods is evaluated using NS-2 simulator in terms of convergence rate, aggregation cycles, average packet drops, transmission cost and network lifetime. Finally, the simulation results establish the validity and efficiency of our approach.

Wireless mobile networks [3] (WSNs) are more likely to be d-distributed asynchronous systems. In this paper, we investigate the achievable data collection capacity of realistic distributed asynchronous WSNs. Our main contributions include five aspects. First, to avoid data transmission interference, we derive an $\Re 0$-proper carrier-sensing range ($\Re 0$-PCR) under the generalized physical interference model, where $\Re 0$ is the satisfied threshold of data receiving rate. Taking $\Re 0$-PCR as its carrier-sensing range, any mobile node can initiate a data transmission with a guaranteed data receiving rate. Second, based on $\Re 0$-PCR, we propose a Distributed Data Collection (DDC) algorithm with fairness consideration. Theoretical analysis of DDC surprisingly shows that its achievable network capacity is order-optimal and independent of network size. Thus, DDC is scalable. Third, we discuss how to apply $\Re 0$-PCR to the distributed data aggregation problem and propose a Distributed Data Aggregation (DDA) algorithm. The delay performance of DDA is also analyzed.

Yih-Chun Hu, Adrian Perrig and David B. Johnson [4], as mobile ad hoc network applications are deployed; security emerges as a central requirement. In this paper we introduce the wormhole attack, a severe attack in ad hoc networks that is particularly challenging to defend against. The wormhole attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and retransmits them there into the network. The wormhole attack can form a serious threat in wireless networks, especially against many ad hoc network routing protocols and location-based wireless security systems. For example, most existing ad hoc network routing protocols, without some mechanism to defend against the wormhole attack, would be unable to find routes longer than one or two hops, severely disrupting communication. We present a new, general mechanism, called packet leashes, for detecting and thus defending against wormhole attacks, and we present a specific protocol, called TIK, that implements leashes.

III. Proposed System

The two metrics to evaluate the performance of the clustering with hybrid CS proposed in this paper: the number of transmissions which is required to collect data from mobiles to the sink and the reduction ratio of transmissions (reduction ratio for short) of our method compared with other methods.

Four other data collection methods are considered. In the clustering without CS method, the same cluster structure to our method is used, but CS is not used. In the shortest path tree (SPT) without CS, the shortest path tree is used to collect data from mobiles to the sink.

In this paper, we propose a clustering method that uses the hybrid CS for Mobile ad-hoc Networks. The mobile nodes are organized into clusters. Within a cluster, nodes transmit data to the cluster head (CH) without using CS. A data gathering tree spanning all CHs is constructed to transmit data to the sink by using the CS method. One important issue for the hybrid method is to determine how big a cluster should be. If the cluster size is too big, the number of transmissions required to collect data from mobile nodes within a cluster to the CH will be very high. But if the cluster size is too small, the number of clusters will be large and the data gathering tree for all CHs to transmit their collected data to the sink will be large, which would lead to a large number of transmissions by using the CS method.

In this regard, we first propose an analytical model to find the optimal size of clusters that can lead to minimum number of transmissions. Then, we propose a k-means clustering algorithm based on the results obtained from the analytical model.

Advantage

- Usage of Mobile Ad-hoc Networks
- Applied k-means Clustering Method.
- Improved security features
- There is Intrusion Detection System with Hybrid Model with both Signature based and Anomaly based methods.

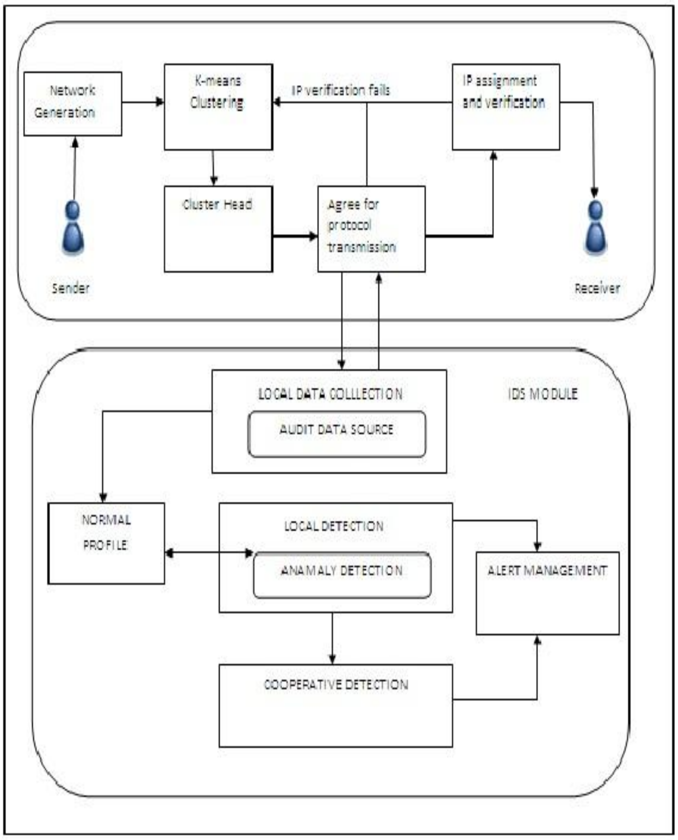

Figure 2 Our Proposed System Model

IV. Implementation

There are five modules involved in the proposed work for secure data transmission in MANET’s from BOTNET attacks.

□ Network formation
□ K-means Clustering
□ Cluster head election
□ Secure Transmission
□ Performance evaluation

Network Topology

The mobile nodes are randomly distributed in a sensing field. We are using mobile ad hoc network (MANET). This is the infra-structure-less network and a node can move independently. In a MANET, each node not only works as a host and also acts as a router. We can find the communication range for all nodes. Every node communicates only within the range. If suppose any node out of the range, node will not communicate those nodes.

Cluster head election

Given the geographic location of the central point of a cluster-area, the mobile node that is the closest to the central point will become the CH. Since the mobile nodes do not know who is the closest to the central point of a cluster area, and we do not know if there is a mobile node falling into the close range of the central point, we let all nodes within the range of Hr from the center be the CH candidates of the cluster, where r is the transmission range of mobiles. The value of H is determined such that there is at least one node within H hops from the central point of a cluster. To elect the CH, each candidate broadcasts a CH election message that contains its identifier, its location and the identifier of its cluster. The CH election message is propagated not more than 2H hops. After a timeout, the candidate that has the smallest distance to the center of the cluster among the other candidates becomes the CH of the cluster. In the extreme case that no mobile node falls within H hops from the central point so that there is no CH for this cluster-area, the nodes in this cluster area accept the invitation from neighbouring CHs and become members of other clusters. Thus, no node will be left out of the network.

K-means Clustering:

After a CH is elected, the CH broadcasts an advertisement message to other mobile nodes in the mobile field, to invite the mobile nodes to join its cluster. An advertisement message carries the information: the identifier and location of the CH, and the number of hop that the message has travelled. The hop count is initialized to be 0. When a mobile node receives an advertisement message, if the hop count of message is smaller than that recorded from the same CH, it updates the information in its record including the node of previous hop and the number of hop to the CH, and further broadcasts the message to its neighbor nodes; otherwise, the message is discarded. After the advertisement of CH is complete, each non-CH node decides which cluster it joins. The decision is based on the number of hops to each CH. The routing from a mobile node to its CH follows the reverse path in forwarding the advertisement message.

Performance Evaluation

In this module, we can evaluate the performance of simulation. We are using the X-graph for evaluate the performance. We choose the four evaluation metrics: Packet delivery ratio – it is the ratio of the number of packet received at destination and number of packet sent by the source, Packet loss – the total number of the packet losses, during the data transmission, End-to-End delay – the average time taken for a packet to be transmitted from the source to destination, Throughput – number of data received by the destination without any losses

V. Algorithm Used

TECHNIQUE USED:

IDS Type:

Network based Intrusion Detecion System (NIDS)

IDS Technique:

Anamoly Based Intrusion Detection System

PROPOSED ALGORITHM:

Training:

Step 1: Select the number of nodes, n, for the complete system.

Step 2: Identify features common to n layers.

Step 3: Classify the common features

Step 4: Perform feature selection specific to each layer

Step 5: Plug in the trained models sequentially such that only the connections labelled as normal are passed to the next layer.

Testing:

Step 6: For each (next) test instance perform Steps 8 to 11.

Step 7: Test the instance and label it either as attack or normal.

Step 8: If the instance is labelled as attack, block it and identify it as an attack represented by the layer name at which it is detected and go to Step 7. Else pass the sequence to the next layer.

Step 9: If the current layer is not the last layer in the system, test the instance and go to Step 9. Else go to Step 11.

Step 10: Test the instance and label it either as normal or as an attack. If the instance is labelled as an attack, block it and identify it as an attack corresponding to the layer name

VI. CONCLUSION

MANET technologies are becoming successful solutions in many applications that allow wireless devices to communicate with each other and access the classified information reliably by exploiting external intermediate mobile nodes. CP-ABE is a scalable cryptographic solution to the access control and secures data retrieval issues. But in this APE encryption technique as limited in Clustering Methods, No Improved security features and there is no Intrusion Detection System. In this paper, we proposed an efficient and secure data transmission method using Hybrid Intrusion Detection system for to address the BOTNET attacks in Mobile ad-hoc networks. The inherent key escrow problem is resolved such that the confidentiality of the stored data is guaranteed even under the hostile environment where key authorities might be compromised or not fully trusted. In addition, the fine-grained key revocation can be done for each attribute group. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data in Mobile Networks.

References

[1] A. Lewko and B. Waters, “Decentralizing attribute-based encryption,”Cryptology Print Archive: Rep. 2010/351, 2010.

[2] S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute based data sharing with attribute revocation,” in Proc. ASIACCS, 2010, pp. 261–270.

[3] S. S.M. Chow, “Removing escrow from identity-based encryption,” inProc. PKC, 2009, LNCS 5443, pp. 256–276.

[4] A. Boldyreva, V. Goyal, and V. Kumar, “Identity-based encryption with efficient revocation,” in Proc. ACM Conf. Comput.Commun. Security,2008, pp. 417–426.

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proc.ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

[6] S. Rafaeli and D. Hutchison, “A survey of key management for secure group communication,”Comput. Surv., vol. 35, no. 3, pp. 309–329, 2003.

[7] S. Mittra, “Iolus: A framework for scalable secure multicasting,” in Proc. ACM SIGCOMM, 1997, pp. 277–288

[8] X. Liang, Z. Cao, H. Lin, and D. Xing, “Provably secure and efficient bounded ciphertext policy attribute based encryption,” inProc. ASIACCS, 2009, pp. 343–352.

[9] M. Chase and S. S. M. Chow, “Improving privacy and security in multi-authority attribute-based encryption,” inProc. ACM Conf. omput. Commun. Security, 2009, pp. 121–130.

[10] M. Belenkiy, M. Chase, M. Kohlweiss, and A. Lysyanskaya, “P-signatures and noninteractive anonymous credentials,” inProc. TCC, 2008, LNCS 4948, pp. 356–374