IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

D2c2 - Dynamic and Desertion Based Credible Communication in Mobile Ad-Hoc Networks

P. Saranya[1], Dr. S. Yamini[2]

M.Phil Scholar, Department of Computer Science, RVS College of Arts and Science (Autonomous), Coimbatore[1]

M.Sc (cc), M. Phil., Ph.D., Director (Academic) School of Computer Studies[2]

Abstract: Mobile ad-hoc networks (MANETs) assume that mobile nodes voluntary cooperate in order to work properly. This cooperation is a cost-intensive activity and some nodes can refuse to cooperate, leading to a selfish node behavior. Thus, the overall network performance could be seriously affected. Many message authentication schemes have been developed, based on either symmetric-key cryptosystems or public-key cryptosystems. In our proposed frame work, use hybrid techniques are clustering scheme and RKP for improve network life time and security In this paper, we propose and evaluate an energy efficient clustering scheme for periodical data gathering applications in WSNs. In the cluster head election phase, a constant number of candidate nodes are elected and compete for cluster heads according to the node residual energy. The competition process is localized and without iteration, thus it has much lower message overhead. The method also produces a near uniform distribution of cluster heads. And this cooperation is a cost-intensive activity and some nodes can refuse to cooperate, leading to a selfish node behavior. Many message authentication schemes have been developed, based on either symmetric-key cryptosystems or public-key cryptosystems. In our proposed using RKP (Random Key Pre-distribution) .RKP schemes have several variants. Their system works by distributing a key ring to each participating node in the sensor network before deployment. We propose a key management scheme that relies on probabilistic key sharing among nodes within the sensor network. Therefore, the nodes build up the network using their secret keys after deployment, that is, when they reach their target position.

Keywords: Mobile ad hoc networks, Clustering, Public-key cryptosystems, Key Pre-distribution, Mobile nodes, Secure Authentication.

I.INTRODUCTION

As the wireless network technology exploded, it has opened a new view to users and expanded the information and application sharing very conveniently and fast. Mobile ad hoc networks (MANETs) use wireless technology without a pre-existing infrastructure (access points). As the name states, MANETs consists of mobile nodes, which can vary from notebooks, PDAs to any electronic device that has the wireless RF transceiver and message handling capability.

Mobility and no-infrastructure forms the basis of this network type Mobility gives maximum freedom to users, as they can be connected to the network, whether they are fixed or moving, unless they are in the range of the network.

Also, it is highly dynamic, as the new nodes come, they can be connected to the network very easily. Unlike the fixed networks or traditional wireless networks, MANETs don't need any infrastructure to create and maintain communication between nodes. In previous works, DSR involves two main processes: route discovery and route maintenance. To execute the route discovery phase, the source node broadcasts a Route Request (RREQ) packet through the network. If an intermediate node has routing information to the destination in its route cache, it will reply with a RREP to the source node. When the RREQ is forwarded to a node, the node adds its address information into the route record in the RREQ packet. When destination receives the RREQ, it can know each intermediary node's address among the route. The destination node relies on the collected routing information among the packets in order to send a reply RREP message to the source node along with the whole routing information of the established route. This property provides the ability to create a network in very unexpected and urgent situations very quickly, also without any extra cost. Mobile ad-hoc networks (MANETs) assume that mobile nodes voluntary cooperate in order to work properly. This cooperation is a cost-intensive activity and some nodes can refuse to cooperate, leading to a selfish node behavior. Thus, the overall network performance could be seriously affected. Many message authentication schemes have been developed, based on either symmetric-key cryptosystems or public-key cryptosystems. . In This Project we used RKP (Random Key Pre-distribution).

We propose a key pre-distribution scheme that relies on probabilistic key sharing among nodes within the sensor network. Key pre-distribution is the method of distribution of keys onto nodes before deployment. Therefore, the nodes build up the network using their secret keys after deployment, that is, when they reach their target position.

DOI10.17148/IJARCCE.2016.510107

II.RELATED WORKS

In previous many works, discussed and used key distribution and authentication schemes for secure data sharing and detect malicious nodes in networks. Now here we discuss some works for network detection and prevention.

Cooperative Bait Detection Scheme, in this previous scheme used DSR protocol. Here presented a mechanism to detect malicious nodes launching black/gray hole attacks and cooperative black hole attacks. It integrates the proactive and reactive defense architectures, and randomly cooperates with a stochastic adjacent node. By using the address of the adjacent node as the bait destination address, it baits malicious nodes to reply RREP and detects the malicious nodes by the proposed reverse tracing program and consequently prevents their attacks.

With recent performance advancements in computer and wireless communications technologies, advanced mobile wireless computing is expected to see increasingly widespread use and application, much of which will involve the use of the Internet Protocol (IP) suite. The vision of mobile ad hoc networking is to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes.

In another process proposes a mesh-based multicast protocol, called centered protocol for unified multicasting through announcements (CPUMA), that achieves comparable reliability as existing mesh-based multicast protocols, however, with significantly much less data overhead. In CPUMA, a distributed core-selection and maintenance algorithm is used to find the source-centric center of a shared mesh.

Here presented a protocol for routing packets between wireless mobile hosts in an ad hoc network. Unlike routing protocols using distance vector or link state algorithms, our protocol uses dynamic source routing which adapts quickly to routing changes when host movement is frequent, yet requires little or no overhead during periods in which hosts move less frequently.

Then TBONE protocol to implement the key networking schemes for such a Mobile Backbone Network (MBN). It includes combined network layer operation, i.e. mobile backbone network topological synthesis, and MAC layer resource allocation schemes. The TBONE protocol serves lo allocate resources across the network to ensure that user applications are granted acceptable quality-of-service (QoS) performance, while striving to ensure a highly ,survivable and robust back hole oriented networking architecture.

This proposed technique works as follows. Initially a backbone network of trusted nodes is established over the ad hoc network. The source node periodically requests one of the backbone nodes for a restricted (unused) IP address. If any of the routes responds positively with a RREP to any of the restricted IP then the source node initiates the detection procedure for these malicious nodes.

In the present studies it is proposed a novel scheme named 2ACK which provides an add-on technique for routing schemes that detects the routing misbehavior and to overcomes their adverse effect. The performance of the schemes analyzed and simulated and 95% packet delivery ratio were achieved when 40% misbehaving nodes were present in the MANETs.

III. PROPOSED SYSTEM: DYNAMIC AND DESERTION

This scheme is secure against adaptive chosen-message attacks. Preventing or detecting malicious nodes launching gray hole or collaborative black hole attacks is a challenge. This paper attempts to resolve this issue by designing a dynamic source routing (DSR)-based routing mechanism, which is referred to as the RKP (Random Key Pre-distribution) that integrates the advantages of both proactive and reactive defense architectures.

Our RKP method implements a reverse tracing technique to help in achieving the stated goal. This cooperation is a cost-intensive activity and some nodes can refuse to cooperate, leading to a selfish node behavior. Many message authentication schemes have been developed, based on either symmetric-key cryptosystems or public-key cryptosystems.

In our proposed we using RKP (Random Key Pre-distribution) .RKP schemes have several variants. Their system works by distributing a key ring to each participating node in the sensor network before deployment. We propose a key management scheme that relies on probabilistic key sharing among nodes within the sensor network. Key management is the method of distribution of keys onto nodes before deployment.

- We having shared key scheme.
- Establishment for path key.
- Each node broadcasts a key identifier list.
- Revocation of a compromised node is very important in key distribution scheme.
- Separate privacy key each ring in network.

Cluster Formation
The nodes energy is the most important issue because the nodes are small in size thus making battery replacement unpractical and impossible. Therefore, it is more practical to save energy and prolong the network lifetime by improving the routing algorithm.

Cluster based hierarchical routing protocol is an energy efficient routing protocol. In the cluster routing, the sensor nodes will be divided into a few groups with one cluster

DOI10.17148/IJARCCE.2016.510107

head elected for each group. The cluster head collects data from member nodes in the same cluster and aggregates the collected data so that it can be transmitted to the base station.

Set Protocol
Secure data Transmission protocol for WSNs. The protocol is designed with the same purpose and scenarios for CWSNs with higher secure and efficiency.

The proposed scheme operates similarly to the previous Key management, which has a protocol initialization prior to the network deployment and operates in rounds during communication. We introduce the protocol initialization, and describe the key management of the protocol by using the scheme, and the protocol operations afterwards. This method used for secure access and data transmission to nearby sensor nodes, by authenticating with each other.

Key Management for Security
In this module, security is based on the multiplicative group. The corresponding private pairing parameters are preloaded in the sensor nodes during the protocol initialization. In this Module, the key cryptographies used in the protocol to achieve secure data transmission, which consist of symmetric and asymmetric key based security.

This scheme enables the intermediate nodes to authenticate the message so that all corrupted message can be detected and dropped to conserve the sensor power. It proposes an efficient key management framework to ensure isolation of the compromised nodes.

Signing of Signature & Verification
In this process a secure access and data transmission to nearby sensor nodes, by authenticating with each other. Each node haves each signatures to authenticate the node, sender and receiver. And key is created for every data and sent to both receiver and the sender nodes.

The signature is used for this signature generation and key generation. It checks whether the information is coming from secure sender and from the correct path. After authentication, the receiver receives the information through the secure nodes.

IV.RANDOM KEY PRE-DISTRIBUTION

Generally, a key establishment scheme has nothing to do with the routing protocol. However, the path in lots of RKPD schemes, such as the basic scheme, is set up through a routing protocol.

That is, a customized routing protocol needs to be used along with those key distribution schemes, which will seriously affect the portability of those RKPD schemes.

Moreover, the number of hops of the path may increase because the adjacent nodes in the path must be logically connected. In fact, the total amount of computation cost for deciding whether a shared key exists in key rings of two adjacent nodes is also very huge because the routing process may involve many nodes.

Our scheme is less competitive in terms of the computation and communication complexity analysis. However, the execution time of a path key establishment for our scheme is slightly less than that of the basic scheme in the simulation. The reason is that, the complexity does not include the extra traffic and calculations that are caused by the customized routing protocol in the basic scheme.

The Scheme
A new random key pre-distribution scheme is described in this section. The scheme also includes three phases:
(1) Key pre-distribution,
(2) Shared key discovery, and
(3) Path key establishment.

Key pre-distribution: Before the deployment of nodes, for each node, a control center (CC) randomly chooses a key ring and loads it into the node. The CC randomly generates keys and assigns a unique key identifier to each; those keys and the corresponding identifiers compose a key pool.

The CC chooses a deterministic algorithm to decide the key identifiers allocated to each node on the input of the node’s identifier. For each node, the CC inputs its identifier into and output distinct values between and, denoted by. At last, the CC draws keys whose key identifiers are. Those keys and the corresponding key identifiers compose a key ring which is loaded into node.

Shared key discovery: After the deployment of nodes, each node creates its own neighbor list. Each node broadcasts its identifier and records the received identifiers, denoted by. For each node, node runs the procedure and generates the key identifier set of nodes. If there is a common key identifier in such set and its own key ring, they are logically connected. Then node adds a record involving the node identifier and the same key identifier to its neighbor list.

Path key establishment: Node wants to establish a path key with node. If they are in wireless communication range and have a shared key, that is, they are on each other’s neighbor list the shared key can be used as the path key. Else, randomly generates a path key and encrypts with some key in key ring.
The cipher text, denoted by, together with the identifier of the encryption key is sent to on a physical connected path founded by a routing protocol. Finally, finds the encryption key corresponding to the received key identifier and decrypts CT to obtain. The following procedure explains how can find an encryption key which belongs to key ring.

DOI10.17148/IJARCCE.2016.510107

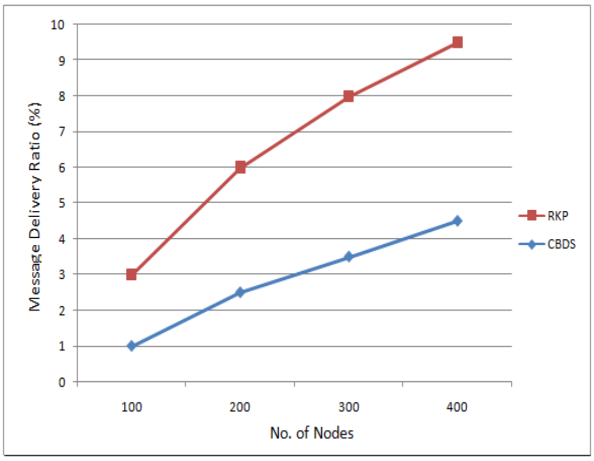
V.PERFORMANCE ANALYSIS

This study used ns-2 as the network simulator and conducted numerous simulations to evaluate the network performance. All sensor nodes are randomly scattered with a uniform distribution. Randomly select one of the deployed nodes as the source node. The location of the sink is randomly determined. This study evaluates the routing performance under scenarios with different numbers of sensor nodes.

This study evaluates the following main performance metrics:

1) Message delivery ratio: is the ratio of the number of report messages the sink receives to the total number of report messages the source node sends.
2) Residual energy: measures the mean value of the residual energy of all alive sensor nodes when simulation terminates.
3) Delivery latency: means the time delay experienced by the source node while transmitting a report message to the sink.

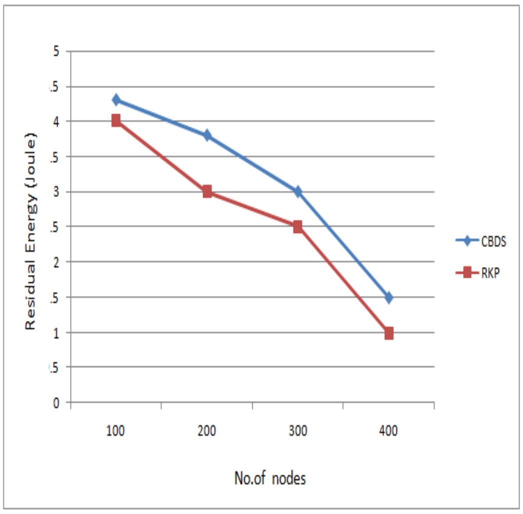
Message Delivery Ratio:



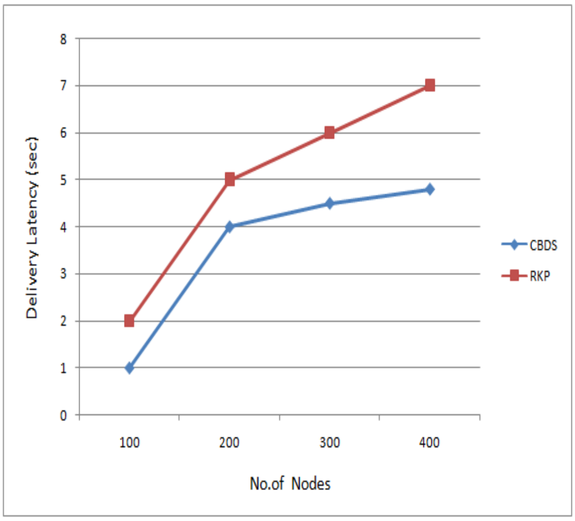
Above graph compares the simulation results of message delivery ratios of the original CBDS and RKP the message delivery ratios of this mechanisms decreases, as Ns increases. Because increasing Ns increases the number of packets in the network, the probability of packet collisions also increases. In this case, the discovered routing path is broken, and the clustering mechanism must reconstruct the cluster structure. This reconstruction may lead to additional energy consumption of sensor nodes, thereby decreasing the packet delivery ratio.

Residual Energy:

Following graph provides a comparison of the energy consumption results of four clustering mechanisms under scenarios with different nodes. In general, the clustering mechanism generates more clusters as the number of Ns increases. Sensor node consumes more energy in clustering thereby decreasing the residual energy. Note that the increasing Nreq will increase the report frequency. Sensor nodes have to consume additional battery power to transmit the increased number of report messages. This leads to a reduction of the residual energy of the nodes in the network.



Delivery Latency:



Above graph shows the average delivery latency of proposed RKP mechanisms under scenario with different N s and Nreq. As Ns increases, more data are generated and the length of the discovered routing path also increases. This leads to along delivery latency, as illustrated in above Fig. In general, the nodes along the routing path are likely to exhaust their battery power quickly when Nreq increases.

This may cause cluster reconstruction to determine a new path, thereby increasing the delivery latency. In clustering, node death and poor link quality result in reconstruction of clusters and retransmission of report messages, respectively. The reconstruction and retransmission generate along message latency.

DOI10.17148/IJARCCE.2016.510107

VI.CONCLUSION

In this paper, we have proposed a new mechanism (called the RKP) for detecting malicious nodes in MANETs under collaborative black hole attacks. Our simulation results revealed that we use RKP (Random Key Pre-distribution). We propose a key pre-distribution scheme that relies on probabilistic key sharing among nodes within the sensor network. Key pre-distribution is the method of distribution of keys onto nodes before deployment. This cooperation is a cost-intensive activity and some nodes can refuse to cooperate, leading to a selfish node behavior. Many message authentication schemes have been developed, based on either symmetric-key cryptosystems or public-key cryptosystems.

REFERENCES

[1] M. Ramkumar, N. Memon, R. Simha, “Pre-Loaded Key Based Multicast and Broadcast Authentication in Mobile Ad-Hoc Networks,” Globecom- 2003.

[2] T. Leighton, S. Micali, “Secret-key Agreement without Public-Key Cryptography,”Advances in Cryptology - CRYPTO 1993, pp 456-479, 1994.

[3] R. Blom, “An Optimal Class of Symmetric Key Generation Systems,” Advances in Cryptology: Proc. of Eurocrypt 84, Lecture Notes in Computer Science, 209, Springer-Verlag, Berlin, pp. 335-338, 1984.

[4] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, M. Yung, “Perfectly-Secure Key Distribution for Dynamic Conferences,” Lecture Notes in Computer Science, vol 740, pp 471–486, 1993.

[5] T. Matsumoto, M.E.Hellman, “New Directions in Cryptography,” IEEE Transactions on Information Theory, IT-22(6), Dec. 1976, pp.644-654.

[6] P. Erdos, P. Frankl, Z. Furedi, “Families of Finite Sets in which no Set is Covered by the Union of M Others,” Isreal Journal of Mathematics, 51, pp 79–89, 1985.

[7] L. Gong, D.J. Wheeler, “A Matrix Key Distribution Scheme,” Journal of Cryptology, 2(2), pp 51-59, 1990.

[8] C.J. Mitchell, F.C. Piper, “Key Storage in Secure Networks,” Discrete Applied Mathematics, 21 pp 215–228, 1995.

[9] M. Dyer, T. Fenner, A. Frieze and A. Thomason, “On Key Storage in Secure Networks,” Journal of Cryptology, 8, 189–200, 1995.

[10] D. R. Stinson, T. van Trung, “Some New Results on Key Distribution Patterns and Broadcast Encryption,” Designs, Codes and Cryptography, 14 (3) pp 261–279, 1998.

DOI10.17148/IJARCCE.2016.510107