An Access Authorization Scheme for Mobile Node Based on Risk Evaluation

Jianjun Wang

Information Science and Technology Department, HuNan First Normal University, Changsha 410002, Hunan, China

Jianping Li

School of Computer Science, University of Electronic Science and Technology of China, Chengdu 610054, Sichuan, China

Abstract

Constraints on conventional access delegation rules on mobile nodes (MNs) are simple. The overall fuzzy evaluation is used to integrate the trust risk that is assessed based on the historical access information within a cellular interval, the context risk assessed based on the position temporal and the information leakage risk assessed based on the node density and the overlapped area, into the access delegation risk of MNs, so as to expand the access delegation rules for MNs and improves the rules with respect to flexibility and security. Finally, an example is used to validate the risk evaluation process.

Key words: MOBILE NODES, ACCESS AUTHORIZATION, TRUST LEVEL, POSITIONAL TEMPORAL, RISK EVALUATION, FUZZY AGGREGATION

1. Introduction

Mobile node's identity information is often characterized by using credentials for which an authority may be given by authentication. In reality, even the authorized user may possibly misuse or abuse its authority, especially in the distributed environment where management is not stringent [1-3]. The risks assessment is to evaluate risks to a certain level by analyzing the uncertain risk factors, which has found wide use in the distributed environment [4-6]. In the papers [7,8] it is believed that the risks in user trust and the abused authority are present in the distributed environment, and that data mining and the fuzzy judgment may be used to analyze the risk factors both qualitatively and quantitatively, and finally the result is used to compute the risk in user access. Because the identity information contained in credentials, which is static and still, cannot objectively reflect the history of a mobile node nor predict its future, complete reliance on credentials may cause trust risks ($Risk_{tru}$). In light of the characteristics of mobile nodes, the position and the temporal that are used to improve the strategy on access control allows to control user authority in dynamic way, improving the flexibility in security strategy [9-12]. In giving authority to a mobile node, its positional or temporal may not satisfy all constraints. This may lead the position or the

temporal to deviate resulting in possible context risk in the course of authorizing a mobile node ($Risk_{con}$). Where the deviation is bigger, the risk becomes more severe. In addition, since the moving path of a mobile node is random, there are two cases to generate information leaking risks ($Risk_{rev}$): first, a mobile node is authorized at a location where nodes are densely populated so that messages are vulnerable for eavesdropping by any adjacent nodes; second, message-overlapping area exists between cells so that the nodes located with the overlapped area can access to each other crossing areas. The message leaking risk has adverse effect on confidentiality of messages carried on a mobile node. The overall authorization risk consists of the trust risk, the context risk and the message leaking risk ($Risk_{aut}$).

In this paper, the impact of the external characteristics of mobile nodes on the access authorization risk is analyzed. The fuzzy overall evaluation method is proposed to address the trust risk, the context risk and the message leaking risk in order to enhance security in mobile node authorization. The section 2 in the paper describes the basic authorization rule based on the positional and temporal for mobile nodes; Section 3 proposes the evaluation methods appropriately aiming at characteristics of the trust risk, the context risk and the message leaking risk and then uses the fuzzy overall evaluation to calculate the access authorization risk; Section 4 demonstrates the risk evaluation process with an example; finally, Section 5 finally draws a conclusion.

2. Principle on mobile node authorization

It is necessary to verify identity of a mobile node when it enters a cellular zone. Figure 1 shows the access to a cellular zone by a mobile node P, where the line $i — j — k — l — m$ is the moving path of the mobile node P. The cellular zone i is expressed by C_i.

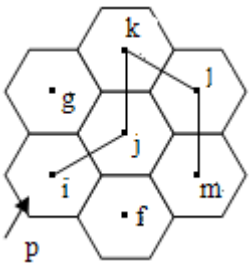

Figure 1. Cellular accessing path of mobile node P

Authorization to the mobile node P is governed by the positional and temporal. $Location(\mathrm{P},d)$ represents the position of the node P at the temporal interval d, $AllocLoc(\mathrm{P})$ represents the set of positions that are allowed to authorize the node P and $AllocDur(\mathrm{P})$ represents the temporal interval when the node P is allowed for authorization.

If the mobile node P is at a position that is allowed to assign authority at the time when it is allowed, then the node P will be given authorization. $Assign(\mathrm{P},d,l)$ is used to express the authorization given to the node P based on the position l and the temporal interval d, and then the access authorization strategy is formulated in Eq.(1) [12].

$$Assign(\mathrm{P},d,l) \Rightarrow (Location(\mathrm{P},d)=l) \wedge (l \in AllocLoc(\mathrm{P})) \wedge (d \subseteq AllocDur(\mathrm{P})) \quad (1)$$

3. Risk evaluation in mobile node authorization

There are three fuzzy overall evaluation models for overall authorization risks including the trust risk, the context risk and the message leaking risk: $\mathrm{M}(\wedge,\vee)$, $\mathrm{M}(\bullet,\vee)$, $\mathrm{M}(\wedge,\oplus)$. Because it is possible that the evaluation criteria in the trust risk, the context risk and the message leaking risk may differ from each other, these evaluation models cannot be directly used to compute the overall authorization risk of a mobile node. The solution is to develop a consistent evaluation criteria for the trust risk, the context risk and the message leaking risk so that they are mutually comparative. It is feasible to normalize risk values.

3.1. Trust risk

It is assumed that the mobile node P interacts with the cell C_i in total numbers of His_i of which Suc_i is the number of successful interactions, Fal_i is the number of failed ones and then $(His_i - Suc_i - Fal_i)$ is the number of interactions which is unknown for success or failure. The credibility Tru_i of the node P at the cell C_i is computed with Eq.(2).

$$Tru_i = Suc_i / His_i \quad (2)$$

The risk value $Risk_i$ of the node P at the cell C_i is calculated with the Eq.(3).

$$Risk_i = 1 - Tru_i \quad (3)$$

3.2. Context risk

When a mobile node P is applying an access authority to the cellular interval C_i, its related-context risk includes the positional deviation risk and the temporal deviation risk.

Mobile node P 's legal authorization position L is any point within the area C_i centering in O_i and in the radius of r_i, i.e. $|L - O_i| \le r_i$. The actual position given an authorization is l. The function $D(l,O_i)$ is used to calculate the distance

between the points l and O_i. If the result is $D(l,O_i) > r_i$, then it is an authorization at an illegal position and the positional deviation ΔL is $|D(l,O_i) - r_i|$; If the result is $D(l,O_i) \le r_i$, then $\Delta L = 0$. The risk arising from the positional deviation is expressed in $Risk_{\Delta L}$. $Risk_{\Delta L}$ should increases monotonically with ΔL and may change in steps. To make $Risk_{\Delta L}$ fall with the risk domain in Table 1, the function Sigmoid may be used to characterize the relation among $Risk_{\Delta L}$, ΔL and r_i, for example in Eq. (4) where k_1 is the gradient, $k_1 > 0$. Deduction of 0.5 is to make $Risk_{\Delta L}$ result be 0 when ΔL is 0.

$$Risk_{\Delta L} = \frac{1}{1+\exp(-k_1 \Delta L / r_i)} - 0.5 \quad (4)$$

It is known from (6) $0 \le Risk_{\Delta L} < 0.5$ is the result of $0 \le \Delta L < \infty$.

Temporal interval for legal authorization to the mobile node P is $[T, T']$ and the actual time interval of authorization is t. In the case of $t < T$ or $t > T'$, it means occurrence of the temporal deviation which is expressed in ΔT. In the case of $t < T$, then $\Delta T = |T - t|$; in the case of $t > T'$, then $\Delta T = |T' - t|$; If $T < t < T'$, then $\Delta T = 0$. The risk arising from the temporal deviation is expressed with $Risk_{\Delta T}$, and based on Eq.(6), similarly one can use the function Sigmoid to characterize the relations among $Risk_{\Delta T}$, ΔT and $[T, T']$, for instance, Eq.(5), where k_2 is the gradient, $k_2 > 0$. $Risk_{\Delta T}$ increases with increase in ΔT.

$$Risk_{\Delta T} = \frac{1}{1+\exp(-k_2 \Delta T / |T - T'|)} - 0.5 \quad (5)$$

It is known from (5) $0 \le Risk_{\Delta T} < 0.5$ is the result of $0 \le \Delta T < \infty$.

Because $Risk_{\Delta L}$ and $Risk_{\Delta T}$, independent of each other, have superposition effect on $Risk_{con}$, the sum of $Risk_{\Delta L}$ and $Risk_{\Delta T}$ is used to represent $Risk_{con}$ as shown in Eq.(6).

$$Risk_{con} = Risk_{\Delta L} + Risk_{\Delta T} \quad (6)$$

It is obvious both $0 \le Risk_{con} < 1$ and $Risk_{con}$ will increase with increased ΔL and ΔT, which have basically the same tendency as the risk value generated from the context deviation for the mobile node. $Risk_{con}$'s threshold is set as 0.5. From the characterization of Eqs (4) and (5), the only possibility for $Risk_{con}$ to exceed the $Risk_{thr}$ is that one of ΔL and ΔT is not 0.

3.3. Message leaking risk

There are two cases for the mobile node P in message leaking risk: The first case is a cross-area eavesdropping within the signal overlapping areas; the second case is mutual eavesdropping between users within one single area. Figure 2 is the sketch of message leaking.

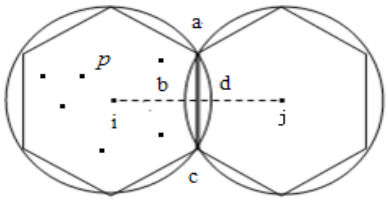

Figure 2. Sketch of message leaking

The first case: As shown in figure 2, the signal-overlapped area between Cells C_i and C_j is S_{abcd}. The bigger the overlapped area is, the greater the message leaking risk. $Risk_{ovp}$ is used to express the cell i's message-leaking risk within the signal-overlapped area, S_i is the cell C_i's area, k_3 is the number of the overlapped areas, $k_3 > 0$, then the relation among $Risk_{ovp}$, S_{abcd} and S_i can be expressed in Eq. (7).

$$Risk_{ovp} = \frac{1}{1+\exp(-k_3 S_{abcd} / S_i)} - 0.5 \quad (7)$$

It is known from Eq.(7) that $Risk_{ovp} \in [0, 0.5)$.

The second case: When the mobile node P is within the authorized cell i, it is possible that its message may be eavesdropped by other nodes nearby resulting in the message leaking risk to adjacent nodes $Risk_{adjo}$. P 's message leaking risk is closely related to the node density within the area. The denser it is, the risk to leak message is severer. For instance, in the public, the node density is in general higher than that in the private places and so the probability in message leaking in the public is higher than that in private places. The number of nodes accessing to the cell i at the time t is M_t and the node density ρ_t is the ratio of M_t and S_i, $\rho_t = M_t / S_i$ in this case. $Risk_{adjo}$ increases with increase in ρ_t and the relation of the risk $Risk_{adjo}$ versus ρ_t is characterized in Eq.(8) where k_4 is the gradient, $k_4 > 0$. $Risk_{adjo} \in [0, 0.5)$.

$$Risk_{adjo} = \frac{1}{1+\exp(-k_4 \rho_t)} - 0.5 \quad (8)$$

$Risk_{rev}$ is dependent jointly on $Risk_{ovp}$ and $Risk_{adjo}$. Because $Risk_{ovp}$ and $Risk_{adjo}$ have positively increasing effect on $Risk_{rev}$, $Risk_{rev}$ can be calculated by summing $Risk_{ovp}$ and $Risk_{adjo}$ as shown in Eq.(9).

$$Risk_{rev} = Risk_{ovp} + Risk_{adjo} \quad (9)$$

$Risk_{rev} \in [0,1)$ is obtained from $Risk_{ovp} \in [0,0.5)$ and $Risk_{adjo} \in [0,0.5)$, and the $Risk_{rev}$ threshold is 0.5.

4. Overall evaluation of authorization risk

If the impact of the trust risk, the context risk and the message leaking risk on the mobile node's overall authorization risk is not considered, Zadeh operator "∧" or "∨"can be used directly to calculate the over risk; if their respective impact is considered, it is necessary to introduce the weights for each risk value, either by weighting and then use "∧" and "∨" to calculate the over authorization risk or by weighting and then summing. The overall authorization risk threshold is the median 0.35 of the smaller interval $[0.2,0.5)$.

Though the risk factors in the trust risk, the context risk and the message leaking risk are different, they are not independent of each other. The size of the trust risk may affect the sizes of the context risk and the message leaking risk. If a mobile node's trust risk is small, the loss may be small even at position where the context risk or the message leaking risk is big. The context risk and the message leaking risk repels mutually to some degree. Where ΔL is not 0, there exists message leaking risk for a mobile node at its position, even though it is not within the target cellular interval; where ΔL is 0, it is certain that the context risk would not be beyond the threshold.

In view of the relation between the trust risk, the context risk and the message leaking risk present in the mobile node P, it is appropriate to calculate using the weighted summing risk aggregation.

The weights $A = (a_1, a_2, a_3)$ and $a_1 + a_2 + a_3 = 1$, where a_1, a_2 and a_3 are weights of $Risk_{tru}$, $Risk_{con}$ and $Risk_{rev}$ respectively. The formula to compute the overall authorization risk $Risk_{aut}$ is Eq.(10).

$$Risk_{aut} = (a_1, a_2, a_3)\begin{bmatrix} Risk_{tru} \\ Risk_{con} \\ Risk_{rev} \end{bmatrix} \quad (10)$$

The basic condition for the node P to be given an authorization is that all the trust risk, the context risk and the message leaking risk as well as the overall authorization risk are less than the threshold. The Eq.(1) is modified as Eq.(11).

$$Assign(\mathrm{P}, d, l) \Rightarrow (Location(\mathrm{P}, d) = l) \wedge (l \in AllocLoc(\mathrm{P})) \wedge (d \subseteq AllocDur(\mathrm{P}))$$
$$\wedge (Risk_{tru} < Risk_{thr}) \vee ((Risk_{\Delta L} < Risk_{thr}) \wedge (Risk_{\Delta T} < Risk_{thr}) \wedge (Risk_{acc} < Risk_{thr})) \quad (11)$$

Mobile node P 's overall authorization risk evaluation flow chart is shown in Figure 3.

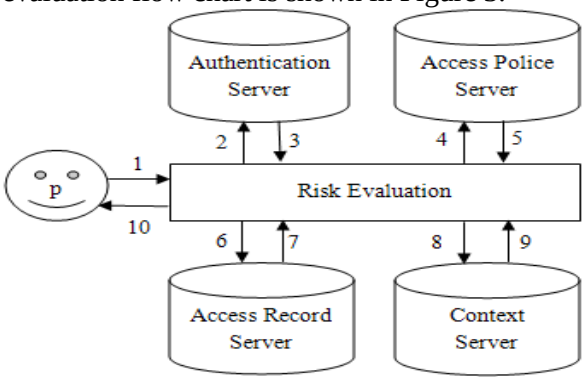

Figure 3. Mobile node P 's authorization risk evaluation

The steps in evaluation of risk in mobile node P authorization:

Step 1: Mobile node P request to access and submit its credential.

Step 2: The Risk Evaluation module submits P 's credential to the authentication server for authentication;

Step 3: The authentication server returns the result to the Risk Evaluation module; if the identity authentication failed, its access is denied and goes to;

Step 4: If the identity authentication passed, the Risk Evaluation module requests to access Access Policy Server to query the access policies including the allowed access authority, the locations and time duration;

Step 5: Risk Evaluation module receives the access policies from Access Policy Server and then requests to evaluate based on the access policies the trust risk, the context risk, the message leaking risk and the overall authorization risk;

Step 6: Risk Evaluation module requests to access the Access Report Server to query the historical information in cells that P has accessed to and the number of nodes in the current cell;

Step 7: Based on the historical access information in cells Risk Evaluation module calculates the credibility and the risk value, and determine whether the trust risk reaches the threshold, and denies its access and goes to Step 10 if the threshold reached;

Step 8: Risk Evaluation module requests the Context Server to query the current position and time of the mobile node P, the center positions of the cell where it is in and the cells nearby as well as the cell radius;

Step 9: Based on the access policies and the context information Risk Evaluation module

calculates the context risk; based on access policies, the context information and the numbers of nodes accessing to the current cell, calculates the message leaking risk. It then determines whether the context risk and the message leaking risk reach the threshold, and if reached, denies its access and goes to Step 10; if not reached, it subsequently calculates the overall authorization risk and determines whether it reaches the threshold, and if reached, denies its request and goes to Step 10;

Step 10: Return the evaluated result to the mobile node P..

5. Application example

According to Figure 2, the mobile node P is accessing to the cell C_m. Exemplify this with the doctor diagnosis. The hospital supports its doctors to do their work using the internal cellular network and the doctor's diagnosis room is within a cellular network C_m as per the network design. The doctors use the mobile terminals to query patient's information and give diagnostic schemes. In principle, doctors are allowed to do their jobs inside their respective office during the work hours $[9:00 \sim 11:00]$ only. The possibility exists that any doctors may do jobs beyond these requirements but which may cause risks. For instance, when a doctor is querying patient's information it may leak out a patient's private information; if he (she) is querying early than the prescribed time, the patient data may not be updated; if later than the prescribed time, the patient's illness may have changed. Therefore, it is necessary to determine the risks possibly present in doctor's doing their jobs and consideration of over access risks is more secure and effective than consideration of one aspect only.

The cell C_m's center O_m is $(0,0)$ and radius r_m is 3. $Risk_{tru}$ is 0.188.

Great changes are found for the context of the mobile node and so three states are discussed here: the normal access, the abnormal-but-allowed access and the abnormal-and-denied access.

Normal access: according to Figure 2, if a doctor requests to access at $\Delta L = 0$ and $\Delta T = 0$ which fall within the normal access, then $Risk_{\Delta L} = 0$, $Risk_{\Delta T} = 0$ and $Risk_{con} = 0$.

Abnormal-but-allowed access: if a doctor requests to access at the position $(3,4)$ at the time $12:00$, $k_1 = 1$, $k_2 = 1$. Then, $Risk_{\Delta L} \approx 0.17$ is calculated from Eq.(4); $Risk_{\Delta T} = 0.12$ is calculated form Eq.(5); $Risk_{con} = 0.29$ is obtained from Eq.(6). Since $Risk_{con}$ does not reach the threshold, its access is approved.

Abnormal-and-denied access: If a doctor requests to access at the position $(4,6)$ at the time $13:00$, then $Risk_{\Delta L} \approx 0.33$, $Risk_{\Delta T} \approx 0.23$, $Risk_{con} = 0.56$. $Risk_{con}$ reaches the threshold, so access denied.

Overlapped area S_{abcd} is 0.3. Since there are 3 cells near C_m, so $k_3 = 3$; $Risk_{ovp} = 0.01$ is obtained from Eq.(7); Let the number of nodes within the cell is 18 and then $k_4 = 1$ and $Risk_{adjo} = 0.15$ is obtained from Eq.(8). $Risk_{rev} = 0.16$ calculated from Eq.(9) is less than the threshold, so access approved. As for the denied access on $Risk_{rev}$, it is not demonstrated here.

To compute overall authorization risk $Risk_{aut}$ requires the access-allowed values of $Risk_{tru}$, $Risk_{con}$ and $Risk_{rev}$. From the previous analysis, $Risk_{tru}$, $Risk_{con}$ and $Risk_{rev}$ respectively are 0.188, 0.29 and 0.16, corresponding to weights $Risk_{aut}$. The overall authorization risk $Risk_{aut}$ is calculated from Eq.(10), $Risk_{aut} = 0.2102 \approx 0.21$, so access approved.

6. Conclusion

The traditional access policy for mobile node access is to bind the positional and temporal with the authority, and authorization is given only when all constraints are met. Therefore, the authorization policy is rigid. In some special cases, a mobile node has to acquire authority beyond required position or temporal. The context risk evaluation is used to evaluate the need, which allows giving authority as long as the access risk is under control. This improves flexibility of the authorization policy while the security in mobile node access is ensured. The traditional access authorization policy only authenticates the credibility of mobile nodes, and the authenticated node is given authority, while the security in node behavior is ignored. The trust risk evaluation on nodes passing identity authentication is proposed to evaluate its credibility based on its history and calculate the trust risk. Mobile nodes, due to mobility and randomness, are vulnerable in message leaking and so the message leaking risk is proposed to evaluate risk in the environment where a mobile node is located. The fuzzy overall evaluation is used to aggregate the three kinds of risks to obtain the access authorization risk in mobile nodes.

In this paper, the risk evaluation is used to fuzzy-expand the access authorization policy for mobile nodes in order to make it more flexible and secure in mobile node's access authorization.

Acknowledgements

The work was supported by the National Natural Science Foundation of China (61370073).

References

1. Ji M A. (2012) Formal Approach for Risk Assessment in RBAC Systems. J*ournal of Universal Computer Science*, 18(9), p.p.2432-2451.
2. Ian M., Luke D., et al. (2012) Risk-based Security Decisions under Uncertainty. *Proc. of 2nd ACM Conf. on Data and Application Security and Privacy*, New York, USA, p.p.157-168.
3. Elise P. L., Peter B. (2011) Risk: Unexpected Uncertainty, and Estimation Uncertainty: Bayesian Learning in Unstable Settings. *PLoS Computational Biology*, 7(1), p.p. 1-14.
4. Luo J. (2011) Risk based Mobile Access Control (RiBMAC) Policy Framework. *Proc. of Military Communications Conf.*, Baltimore, Maryland, p.p.1448 – 1453.
5. Sharma M., et al. (2012) Using Risk in Access Control for Cloud-assisted HHealth. *Proc. of 2012 IEEE 9th International Conference on Embedded Software and Systems*, Washington, USA, p.p. 1047-1052.
6. Langheinrigh M., Karjoth G. (2010) Social Networking and the Risk to Companies and Institutions. *Information Security Technical Report*, 5(2), p.p.51–56.
7. Celikel E., et al. (2007) Managing Risks in RBAC Employed Distributed Environments. Proc. of the 2007 OTM Confederated International Conference on the Move to Meaningful Internet Systems, Berlin, p.p. 1548-1566.
8. Celikel E., et al. (2009) A Risk Management Approach to RBAC. *Risk and Decision Analysis*, 11, p.p. 21-33.
9. Toahchoodee M., Ray I. (2008) On the Formal Analysis of A Spatio-temporal Role-based Access Control Model. *Proc. of the 22st Annual IFIP WG 11.3 Working Conference on Data and Applications Security*, London, p.p. 17–32.
10. Bertino E., et al. (2005) GEO-RBAC: A Spatially Aware RBAC. *Proc. of the 10th ACM Symposium on Access Control Models and Technologies*, Stockholm, p.p. 29–37.
11. Chandran S. M., Joshi J. B. D. (2005) LoT-RBAC: A Location and Time-Based RBAC Model. *Proc. of the 6th International Conference on Web Information Systems Engineering*, Newyork, p.p. 361–375.
12. Ray I., Toahchoodee M. (2007)A Spatio-Temporal Role-Based Access Control Model. *Proc. of the 21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security*, CA, USA, p.p. 211–226.